F ENT COOPERATION TREAT

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 02 May 2001 (02.05.01)	
International application No. PCT/JP00/05770	**Applicant's or agent's file reference** 900391
International filing date (day/month/year) 25 August 2000 (25.08.00)	**Priority date** (day/month/year) 27 August 1999 (27.08.99)
Applicant HATANAKA, Masayuki et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

26 March 2001 (26.03.01)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Antonia Muller

Telephone No.: (41-22) 338.83.38

Translation

PATENT COOPERATION TREATY

PCT

10/069,112

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 900391	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/JP00/05770	International filing date (*day/month/year*) 25 August 2000 (25.08.00)	Priority date (*day/month/year*) 27 August 1999 (27.08.99)
International Patent Classification (IPC) or national classification and IPC G10K 15/02, G06F 15/00, 17/60, H04L 9/08, 9/10, G06K 19/00, H04H 1/00, G06F 12/04, H04M 3/42, 3/493, 11/08, G10L 19/00, G06F 13/00, H04L 12/22, 12/58		
Applicant FUJITSU LIMITED		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 31 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
26 March 2001 (26.03.01)	08 November 2001 (08.11.2001)
Name and mailing address of the IPEA/JP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP00/05770

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 7-29,31-73, as originally filed
pages _____, filed with the demand
pages 1-6,6/3,30 (19.04.01) 6/1,6/2, filed with the letter of 01 November 2001 (01.11.2001)

☒ the claims:

pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages 1-43 (19.04.01) 44-45, filed with the letter of 01 November 2001 (01.11.2001)

☒ the drawings:

pages 1-56, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

☐ the description, pages _____
☒ the claims, Nos. 46
☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP 00/05770

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-45	YES
	Claims		NO
Inventive step (IS)	Claims	1-45	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-45	YES
	Claims		NO

2. Citations and explanations

Claims 1 to 45

Document 1 (Nikkei Electronics, No. 739, "Kogata Memori Kaado de Ongaku Chosakuken wo Mamoru", March 22, 1999 (22.03.99), pp. 49-53) and Document 2 (JP, 10-106148, A (Toshiba Corp.), April 24, 1998 (24.04.98), entire text; all drawings) are documents that reflect the general state of the art in this technical field and disclose methods for encrypting content data. However, the features outlined below are neither disclosed nor suggested in any of the documents cited in the international search report or in the document newly cited in the international preliminary examination report.

(1) The feature wherein the licence key in the content data supply device is encrypted using the common key transmitted from the terminal and the public encryption key. The feature wherein the above-mentioned key is decrypted using the common key and a confidential decryption key.

(2) The feature wherein the session key generated in the content reproduction unit is encrypted using the common key that has been encrypted by the public encryption key, transmitted to the data storing unit, and said key is used to encrypt the licence key.

13T

PCT

特 許 協 力 条 約

国際予備審査報告

（法第１２条、法施行規則第56条）
〔ＰＣＴ３６条及びＰＣＴ規則70〕

出願人又は代理人の書類記号　９００３９１	今後の手続きについては、国際予備審査報告の送付通知（様式ＰＣＴ／ＩＰＥＡ／４１６）を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０５７７０	国際出願日（日.月.年）　２５．０８．００	優先日（日.月.年）　２７．０８．９９
国際特許分類（ＩＰＣ）Int. Cl' G10K15/02, G06F15/00, G06F17/60, H04L9/08, H04L9/10, G06K19/00, H04H1/00, G06F12/04, H04M3/42, H04M3/493, H04M11/08, G10L19/00, G06F13/00, H04L12/22, H04L12/58		
出願人（氏名又は名称）　富士通株式会社		

１．　国際予備審査機関が作成したこの国際予備審査報告を法施行規則第57条（ＰＣＴ３６条）の規定に従い送付する。

２．　この国際予備審査報告は、この表紙を含めて全部で　3　ページからなる。

☒ この国際予備審査報告には、附属書類、つまり補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関に対してした訂正を含む明細書、請求の範囲及び／又は図面も添付されている。
（ＰＣＴ規則70.16及びＰＣＴ実施細則第６０７号参照）
この附属書類は、全部で　３１　ページである。

３．　この国際予備審査報告は、次の内容を含む。

- I ☒ 国際予備審査報告の基礎
- II ☐ 優先権
- III ☐ 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
- IV ☐ 発明の単一性の欠如
- V ☒ ＰＣＴ３５条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
- VI ☐ ある種の引用文献
- VII ☐ 国際出願の不備
- VIII ☐ 国際出願に対する意見

国際予備審査の請求書を受理した日　２６．０３．０１	国際予備審査報告を作成した日　０８．１１．０１
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｃ　９３７９ 樫本　剛 電話番号　０３－３５８１－１１０１　内線　３５４１

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（１９９８年７月）

国際予[redacted]査報告　　国際出願番[redacted]ＣＴ／ＪＰ００／０５７７０

Ⅰ．　国際予備審査報告の基礎

1．　この国際予備審査報告は下記の出願書類に基づいて作成された。（法第６条（ＰＣＴ１４条）の規定に基づく命令に応答するために提出された差し替え用紙は、この報告書において「出願時」とし、本報告書には添付しない。ＰＣＴ規則70.16, 70.17）

☐ 出願時の国際出願書類

☒	明細書	第 7-29, 31-73	ページ、	出願時に提出されたもの
	明細書	第	ページ、	国際予備審査の請求書と共に提出されたもの
	明細書	第 1-6, 6/3, 30	ページ、	１９．０４．０１ 付の書簡と共に提出されたもの
	明細書	第 6/1, 6/2	ページ、	０１．１１．０１ 付の書簡と共に提出されたもの
☒	請求の範囲	第	項、	出願時に提出されたもの
	請求の範囲	第	項、	ＰＣＴ１９条の規定に基づき補正されたもの
	請求の範囲	第	項、	国際予備審査の請求書と共に提出されたもの
	請求の範囲	第 １－４３	項、	１９．０４．０１ 付の書簡と共に提出されたもの
	請求の範囲	第 ４４－４５	項、	０１．１１．０１ 付の書簡と共に提出されたもの
☒	図面	第 １－５６	ページ/~~図~~、	出願時に提出されたもの
	図面	第	ページ／図、	国際予備審査の請求書と共に提出されたもの
	図面	第	ページ／図、	付の書簡と共に提出されたもの
☐	明細書の配列表の部分	第	ページ、	出願時に提出されたもの
	明細書の配列表の部分	第	ページ、	国際予備審査の請求書と共に提出されたもの
	明細書の配列表の部分	第	ページ、	付の書簡と共に提出されたもの

2．　上記の出願書類の言語は、下記に示す場合を除くほか、この国際出願の言語である。

上記の書類は、下記の言語である＿＿＿＿＿＿語である。

☐ 国際調査のために提出されたＰＣＴ規則23.1(b)にいう翻訳文の言語
☐ ＰＣＴ規則48.3(b)にいう国際公開の言語
☐ 国際予備審査のために提出されたＰＣＴ規則55.2または55.3にいう翻訳文の言語

3．　この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際予備審査報告を行った。

☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際予備審査（または調査）機関に提出された書面による配列表
☐ 出願後に、この国際予備審査（または調査）機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

4．　補正により、下記の書類が削除された。

☐ 明細書　第＿＿＿＿＿＿ページ
☒ 請求の範囲　第 ４６ 項
☐ 図面　図面の第＿＿＿＿＿＿ページ／図

5．☐ この国際予備審査報告は、補充欄に示したように、補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)　この補正を含む差し替え用紙は上記１．における判断の際に考慮しなければならず、本報告に添付する。）

V.　新規性、進歩性又は産業上の利用可能性についての法第１２条（ＰＣＴ３５条(2)）に定める見解、それを裏付ける文献及び説明

1.　見解

新規性（N）	請求の範囲	1－45	有
	請求の範囲		無
進歩性（ＩＳ）	請求の範囲	1－45	有
	請求の範囲		無
産業上の利用可能性（ＩＡ）	請求の範囲	1－45	有
	請求の範囲		無

2.　文献及び説明（ＰＣＴ規則70.7）

請求の範囲１－４５

文献１：日経エレクトロニクス，No.739，「小型メモリ・カードで音楽著作権を守る」，22.3月.1999(22.03.99)，p.49-53

文献２：ＪＰ，１０－１０６１４８，Ａ（株式会社東芝）２４．４月．１９９８（２４．０４．９８）全文全図

は、当該技術分野における一般的技術水準を示す文献であって、コンテンツの暗号化方法についての技術が記載されているが、下記の技術に関しては、国際調査報告で列記した文献、及び国際予備審査報告で新たに引用した文献のいずれにも、記載も示唆もされていない。

（１）コンテンツデータ供給装置におけるライセンスキーを、端末から送信された共通鍵と公開暗号化鍵を用いて暗号化する点。また、上記キーを、共通鍵と、秘密復号鍵を用いて復号化する点。

（２）コンテンツ再生部において生成されたセッションキーを、公開暗号化鍵によって暗号化された共通鍵により暗号化してデータ格納部に送信し、該キーを用いてライセンスキーを暗号化する点。

明細書

データ配信システムおよびそれに用いるデータ供給装置、端末装置ならびに記録装置

技術分野

本発明は、携帯電話等の端末に対して情報を配送するためのデータ配信システムに関し、より特定的には、コピーされた情報に対する著作権保護を可能とするデータ配信システムに関するものである。

背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタル情報を記録した記録媒体を例にとって考えてみると、通常販売されている音楽情報を記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行な

う個人ユーザは、[redacted]ジタル録音機器自体やMD等の媒[redacted]の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

しかも、CDからMDへデジタル信号である音楽情報をコピーした場合、これらの情報がコピー劣化のほとんどないデジタル情報であることに鑑み、1つのMDからさらに他のMDに音楽データをデジタル情報としてコピーすることは、著作権者保護のために機器の構成上できないようになっている。

すなわち、現状においては、デジタル記録媒体であるCDからMDへのコピーは、親から子へのコピーは自由に行なうことができるものの、記録可能なMDからMDへのコピーを行なうことはできない。

そのような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

この場合、情報通信網を通じて公衆に送信される著作物データを、本来受信する権限のないユーザが受信することを防止する必要があるのはもちろんのこと、仮に権限を有するユーザが受信を行なった場合でも、一度受信された著作物が、さらに勝手に複製されることを防止することも必要となる。

発明の開示

本発明の目的は、情報通信網、たとえば携帯電話等の情報通信網を介して著作物データを配信する場合に、正当なアクセス権を有するユーザのみがこのような情報を受信することが可能な情報配信システムを提供することである。

この発明の他の目的は、配信された著作物データが、著作権者の許可なく複製されることを防止することが可能な情報配信システムを提供することである。

係る目的を達成するために本願発明に係るデータ供給システムは、コンテンツデータ供給装置から、暗号化コンテンツデータと暗号化コンテンツデータを復号するためのライセンスキーとのうち少なくともライセンスキーを複数のユーザの各端末に配信するためのデータ配信システムである。

コンテンツデータ供給装置は、第1のインタフェース部と、第1のセッションキー発生部と、セッションキー暗号化処理部と、セッションキー復号部と、第1

のライセンスデ[redacted]暗号化処理部と、第２のライセ[redacted]データ暗号化処理部とを備える。

第１のインタフェース部は、外部との間でデータを授受する。第１のセッションキー発生部は、ライセンスキーの通信ごとに更新される第１の共通鍵を生成する。セッションキー暗号化処理部は、第１の公開暗号化鍵により第１の共通鍵を暗号化して第１のインタフェース部に与える。セッションキー復号部は、第１の共通鍵により暗号化されて返信される第２の共通鍵と第２の公開暗号化鍵を第１の共通鍵に基づいて復号し、第２の共通鍵と第２の公開暗号化鍵を抽出する。第１のライセンスデータ暗号化処理部は、ライセンスキーを、セッションキー復号部により抽出された第２の公開暗号化鍵により暗号化する。第２のライセンスデータ暗号化処理部は、第１のライセンスデータ暗号化処理部の出力をセッションキー復号部により抽出された第２の共通鍵によりさらに暗号化して第１のインタフェース部に与えて供給する。

各端末は、第２のインタフェース部と、データ格納部とを備える。

第２のインタフェース部は、外部との間でデータを授受する。

データ格納部は、コンテンツデータ供給装置から少なくともライセンスキーを受けて格納する。第１の公開暗号鍵は、データ格納部に対して予め定められている。データ格納部は、第１の鍵保持部と、第１の復号処理部と、第２の鍵保持部と、第２のセッションキー発生部と、第１の暗号化処理部と、第２の復号処理部と、第３の鍵保持部と、第３の復号処理部と、記憶部とを備える。

第１の鍵保持部は、第１の公開暗号化鍵によって暗号化されたデータを復号するための第１の秘密復号鍵を保持する。第１の復号処理部は、第１の公開暗号化鍵によって暗号化された第１の共通鍵を受けて、復号処理する。第２の鍵保持部は、第２の公開暗号化鍵を保持する。第２のセッションキー発生部は、第２の共通鍵を生成する。第１の暗号化処理部は、第２の公開暗号化鍵と第２の共通鍵を、第１の共通鍵に基づいて暗号化し、第２のインタフェース部に出力する。第２の復号処理部は、第２の共通鍵によって暗号化され、さらに第２の公開暗号化鍵によって暗号化された、第２のライセンスデータ暗号化処理部からのライセンスキーを受け、第２の共通鍵に基づいて復号する。第３の鍵保持部は、第２の公開暗

号化鍵によって暗号化されたデータを復号するためのデータ格納部ごとに固有な第２の秘密復号鍵を保持する。第３の復号処理部は、第２の公開暗号化鍵によって暗号化されたライセンスキーを受け、第２の秘密復号鍵によりライセンスキーを復号し抽出する。記憶部は、暗号化コンテンツデータとライセンスキーを格納する。

この発明のさらに他の局面に従うと、暗号化コンテンツデータと暗号化データを復号するためのライセンスキーとのうち少なくともライセンスキーを、少なくともライセンスキーを格納可能なデータ格納部を備える複数のユーザの各端末に供給するためのデータ供給装置であって、インタフェース部と、セッションキー発生部と、セッションキー暗号化処理部と、セッションキー復号部と、第１のライセンスデータ暗号化処理部と、第２のライセンス暗号化処理部とを備える。

インタフェース部は、外部との間でデータを授受する。セッションキー発生部は、ライセンスキーの通信ごとに更新される第１の共通鍵を生成する。セッションキー暗号化処理部は、ユーザ端末のデータ格納部に対応して予め定められた第１の公開暗号化鍵により第１の共通鍵を暗号化してインタフェース部に与える。セッションキー復号部は、第１の共通鍵により暗号化されて返信される第２の共通鍵と第２の公開暗号化鍵を復号し抽出する。第１のライセンスデータ暗号化処理部は、暗号化コンテンツデータを復号するためのライセンスキーを、セッションキー復号部により復号された第２の公開暗号化鍵により暗号化する。第２のライセンス暗号化処理部は、第１のライセンスデータ暗号化処理部の出力を第２の共通鍵でさらに暗号化してインタフェース部に与え、各端末に供給する。

この発明のさらに他の局面に従うと、暗号化コンテンツデータと暗号化コンテンツデータを復号するためのライセンスキーとのうち少なくともライセンスキーを複数の記録装置に供給するためのデータ供給装置であって、インタフェース部と、第１のセッションキー発生部と、セッションキー暗号化処理部と、セッションキー復号部と、第１のライセンスデータ暗号化処理部と、第２のライセンス暗号化処理部とを備える。

インタフェース部は、記録装置との間でデータを授受する。接続部は、インタフェース部と記録装置を接続してデータを供給可能である。第１のセッションキ

一発生部は、ライセンスキーの供給ごとに更新される第１の共通鍵を生成する。セッションキー暗号化処理部は、記録装置に対して予め定められた第１の公開暗号化鍵により第１の共通鍵を暗号化してインタフェース部に与える。セッションキー復号部は、第１の共通鍵により暗号化されて接続部に接続された記録装置より入力される第２の共通鍵と第２の公開暗号化鍵を復号し抽出する。第１のライセンスデータ暗号化処理部は、暗号化コンテンツデータを復号するためのライセンスキーを、セッションキー復号部により復号された第２の公開暗号化鍵により暗号化する。第２のライセンス暗号化処理部は、第１のライセンスデータ暗号化処理部の出力を第２の共通鍵でさらに暗号化してインタフェース部に与え、接続部に接続された記録装置に供給する。

この発明のさらに他の局面に従うと、データ供給装置から、暗号化コンテンツデータと暗号化コンテンツデータを復号するためのライセンスキーとのうち少なくともライセンスキーの配信を受けるための端末装置であって、第１のインタフェース部と、データ格納部とを備える。

第１のインタフェース部は、外部との間にデータを授受する。

データ格納部は、ライセンスキーを受けて格納する。データ格納部は、第１の鍵保持部と、第１の復号処理部と、第２の鍵保持部と、第２のセッションキー発生部と、第１の暗号化処理部と、第２の復号処理部と、第３の鍵保持部と、記憶部と、第３の復号処理部とを備える。

第１の鍵保持部は、第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する。第１の復号処理部は、第１の公開暗号化鍵によって暗号化され外部から入力された第１の共通鍵を受けて、復号処理する。第２の鍵保持部は、データ格納部ごとに固有な第２の公開暗号化鍵を保持する。第２のセッションキー発生部は、第２の共通鍵を生成する。第１の暗号化処理部は、第２の公開暗号化鍵と第２の共通鍵を、第１の共通鍵に基づいて暗号化し、第１のインタフェース部に出力する。第２の復号処理部は、第２の公開暗号化鍵によって暗号化され、さらに第２の共通鍵によって暗号化されたライセンスキーを受け、第２の共通鍵に基づいて復号する。第３の鍵保持部は、第２の公開暗号化鍵によって暗号化されたデータを復号化するためのデータ格納部ごとに固

有な第２の秘密復号鍵を保持する。記憶部は、第２の復号処理部の出力を受けて、第２の公開暗号化鍵によって暗号化されたライセンスキーを格納する。第３の復号処理部は、記憶部に格納された第２の公開暗号化鍵によって暗号化されたライセンスキーを受け、第２の秘密復号鍵により復号する。

この発明のさらに他の局面に従うと、データ供給装置から、暗号化コンテンツデータと暗号化コンテンツデータを復号するためのライセンスキーとのうち少なくともライセンスキーの配信を受けるための端末装置であって、第１のインタフェース部と、データ格納部とを備える。

第１のインタフェース部は、外部との間にデータを授受する。

データ格納部は、ライセンスキーを受けて格納する。データ格納部は、第１の鍵保持部と、第１の復号処理部と、第２の鍵保持部と、第２のセッションキー発生部と、第１の暗号化処理部と、第２の復号処理部と、第３の鍵保持部と、第３の復号処理部と、記憶部とを備える。第１の鍵保持部は、第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する。第１の復号処理部は、第１の公開暗号化鍵によって暗号化され外部から入力された第１の共通鍵を受けて、復号処理する。第２の鍵保持部は、データ格納部ごとに固有な第２の公開暗号化鍵を保持する。第２のセッションキー発生部は、第２の共通鍵を生成する。第１の暗号化処理部は、第２の公開暗号化鍵と第２の共通鍵を、第１の共通鍵に基づいて暗号化し、第１のインタフェース部に出力する。第２の復号処理部は、第２の公開暗号化鍵にて暗号化され、さらに第２の共通鍵によって暗号化されたライセンスキーを受け、第２の共通鍵に基づいて復号する。第３の鍵保持部は、第２の公開暗号化鍵によって暗号化されたデータを復号するためのデータ格納部ごとに固有な第２の秘密復号鍵を保持する。第３の復号処理部は、第２の公開暗号化鍵によって暗号化されたライセンスキーを受け、第２の秘密復号鍵により復号する。記憶部は、第３の復号処理部の出力を受けて、ライセンスキーを格納する。

この発明のさらに他の局面に従うと、データ供給装置から暗号化コンテンツデータと暗号化コンテンツデータを復号するためのライセンスキーとのうち少なくともライセンスキーの配信を受けるための端末装置であって、第１のインタフェ

ース部と、コンテンツ再生部と、第２のインタフェース部とを備える。

第１のインタフェース部は、データ供給装置との間でデータを授受する。第２のインタフェース部は、端末装置に着脱可能なデータ格納部と接続する。

コンテンツ再生部は、第４の鍵保持部と、第４の復号処理部と、第３のセッションキー発生部と、第２の暗号化処理部と、第５の復号処理部と、データ再生部とを含む。第４の鍵保持部は、第３の公開暗号化鍵にて暗号化されるデータを復号する第３の秘密復号鍵を保持する。第４の復号処理部は、データ格納部にて第３の公開暗号化鍵によって暗号化された第２の共通鍵を復号し抽出する。第３のセッションキー発生部は、第３の共通鍵を生成する。第２の暗号化処理部は、第４の復号処理部にて復号し抽出した第２の共通鍵に基づいて、第３の共通鍵を暗号化し出力する。第５の復号処理部は、データ格納部にて第３の共通鍵に基づいて暗号化されたライセンスキーを復号し抽出する。データ再生部は、データ格納部に記録された暗号化コンテンツデータを、抽出したライセンスキーにて復号し、再生する。

この発明のさらに他の局面に従うと、記録装置であって、インタフェース部と、記録部と、パラレルデータバスと、第１の鍵保持部と、第１の復号処理部と、第２の鍵保持部と、セッションキー発生部と、第１の暗号化処理部と、第２の復号処理部と、第３の鍵保持部と、第３の復号処理部とを備える。

インタフェース部は、外部との間でデータ授受を行なう。

記録部は、データを記録する。パラレルデータバスは、ｍビット幅（ｍは自然数、ｍ＞１）であって、インタフェース部と記録部間のデータの伝達を行う。

インタフェース部は、複数の端子と、選択手段と、第１の変換手段と、第２の変換手段とを含む。

選択手段は、外部からの入力データのビット幅の切換指令に従って、外部からデータを受ける端子として複数の端子から１個またはｎ個（ｎは自然数、１＜ｎ≦ｍ）の予め定められた端子を選択する。第１の変換手段は、切換指令に応じて、選択された１個の端子を介して外部から与えられたシリアルデータ、またはｎ個の端子を介して、外部から与えられたｎビット幅のパラレルデータをｍビット幅のパラレルデータに変換し、パラレルデータバスへ供給する。第２の変換手段は、

パラレルデータバスからのｍビット幅のパラレルデータをシリアルデータに変換して、複数の端子の予め定められた１個の端子を介して外部へ出力する。

第１の鍵保持部は、第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する。第１の復号処理部は、前記第１の公開暗号化鍵によって暗号化された第１の共通鍵を受けて、前記第１の秘密復号鍵に基づいて復号処理する。第２の鍵保持部は、第２の公開暗号化鍵を保持する。セッションキー発生部は、第２の共通鍵を生成する。第１の暗号化処理部は、前記第２の公開暗号化鍵と前記第２の共通鍵を前記第１の共通鍵に基づいて暗号化し、前記パラレルデータバスを介して前記インタフェース部に出力する。第２の復号処理部は、前記第２の公開暗号化鍵で暗号化され、さらに前記第２の共通鍵にて暗号化されたライセンスキーを受け、前記第２の共通鍵に基づいて復号する。第３の鍵保持部は、前記第２の公開暗号化鍵によって暗号化されたデータを復号化するための前記記録装置ごとに設定された第２の秘密復号鍵を保持する。第３の復号処理部は、前記第２の公開暗号化鍵で暗号化されたライセンスキーを受けて、前記第２の秘密復号鍵に基づいて復号して、前記ライセンスキーを抽出する。前記記録部は、前記暗号化コンテンツデータと前記ライセンスキーを格納する。

図面の簡単な説明

図１は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

図２は、図１に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明する図である。

図３は、図１に示した配信サーバ１０の構成を示す概略ブロック図である。

図４は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

図５は、図４に示したメモリカード１１０の構成を説明するための概略ブロック図である。

図６は、図１および図３～図５で説明したデータ配信システムにおける配信モ

ードを説明するための第１のフローチャートである。

図７は、図１および図３～図５で説明したデータ配信システムにおける配信モードを説明するための第２のフローチャートである。

図８は、携帯電話機１００内においてコンテンツデータを再生し、、音楽として外部に出力するための再生処理を説明するフローチャートである。

図９は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１のフローチャートである。

図１０は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第２のフローチャートである。

図１１は、実施の形態２のメモリカード１２０に対応した音楽サーバ３１の構成を示す概略ブロック図である。

メモリカード１２０の構成が、メモリカード１１０の構成と異なる点は、まず、メモリカード１２０は、このカード独自のセッションキーＫｓ１を発生するセッションキーＫｓ１発生部１４３２を備えることである。

さらに、メモリカード１２０は、セッションキー発生回路１４３２で生成されたセッションキーＫｓ１を、暗号化してデータバスＢＳ３に与えるための暗号化処理部１４３０を備える。

これに応じて、メモリカード１２０は、さらに、再生モードにおいて、携帯電話機１０１の公開暗号化鍵ＫＰｐを受けて保持するＫＰｐ受理部１４０７と、移動モードにおいて、相手方（移動先）の公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）を受けて保持するＫＰｍｅｄｉａ受理部１４０３と、このＫＰｍｅｄｉａ受理部１４０３の出力とＫＰｐ受理部１４０７の出力とを受けて、動作モードに応じていずれか一方を出力する切換えスイッチ１４３６を備える。切換えスイッチ１４３６は、接点ＰｉおよびＰｈとを有し、接点ＰｉはＫＰｐ受理部１４０７と、接点ＰｈはＫＰｍｅｄｉａ受理部１４０３とそれぞれ結合する。暗号化処理部１４３０は、切換えスイッチ１４３６から与えられる公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）または公開暗号化鍵ＫＰｐのいずれかにより、Ｋｓ１発生部１４３２からのセッションキーＫｓ１を暗号化して、データバスＢＳ３に与える。

すなわち、切換えスイッチ１４３６は、配信動作のとき、および移動動作において移動先となっているときは、未使用状態であり、再生動作の時は、接点Ｐｉの側に閉じており、移動動作において移動元となっているときは、接点Ｐｈの側に閉じている。

メモリカード１２０は、さらに、接点Ｐｅ、ＰｆおよびＰｇを有し、復号処理部１４０４から与えられる音楽サーバからのセッションキーＫｓと、Ｋｓ１発生部１４３２の出力と、データバスＢＳ４から与えられる携帯電話機１０１からのセッションキーＫｓとを受けて、動作モードに応じていずれか１つを選択的に出力する切換えスイッチ１４３５を備える。接点Ｐｅには復号処理部１４０４からの出力が、接点ＰｆにはＫｓ１発生部１４３２の出力が、接点Ｐｇにはデータバスバス４がそれぞれ結合している。したがって、暗号化処理部１４０６と復号処理部１４１０は、この切換えスイッチ１４３５から与えられるキーに基づいて、

請求の範囲

1．（補正後）コンテンツデータ供給装置から、暗号化コンテンツデータと前記暗号化コンテンツデータを復号するためのライセンスキーとのうち少なくとも前記ライセンスキーを複数のユーザの各端末に供給するためのデータ供給システムであって、

前記コンテンツデータ供給装置は、

外部との間でデータを授受するための第１のインタフェース部（３５０）と、

前記ライセンスキーの通信ごとに更新される第１の共通鍵を生成する第１のセッションキー発生部（３１４）と、

第１の公開暗号化鍵により前記第１の共通鍵を暗号化して前記第１のインタフェース部に与えるためのセッションキー暗号化処理部（３１６）と、

前記第１の共通鍵により暗号化されて返信される第２の共通鍵と第２の公開暗号化鍵を前記第１の共通鍵に基づいて復号し、前記第２の共通鍵と前記第２の公開暗号化鍵を抽出するセッションキー復号部（３１８）と、

前記ライセンスキーを、前記セッションキー復号部により抽出された前記第２の公開暗号化鍵により暗号化するための第１のライセンスデータ暗号化処理部（３２０）と、

前記第１のライセンスデータ暗号化処理部の出力を前記セッションキー復号部により抽出された前記第２の共通鍵によりさらに暗号化して前記第１のインタフェース部に与えて供給するための第２のライセンスデータ暗号化処理部（８２２）とを備え、

各前記端末は、

外部との間でデータを授受するための第２のインタフェース部と、

前記コンテンツデータ供給装置から少なくとも前記ライセンスキーを受けて格納するためのデータ格納部（１４０）とを備え、

前記第１の公開暗号鍵は、前記データ格納部に対して予め定められており、

前記データ格納部は、

前記第１の公開暗号化鍵によって暗号化されたデータを復号するための第１の

秘密復号鍵を保持する第１の鍵保持部（１４０２）と、

前記第１の公開暗号化鍵によって暗号化された前記第１の共通鍵を受けて、復号処理するための第１の復号処理部（１４０４）と、

前記第２の公開暗号化鍵を保持するための第２の鍵保持部（１４０５）と、

前記第２の共通鍵を生成する第２のセッションキー発生部（１４３２）と、

前記第２の公開暗号化鍵と前記第２の共通鍵を、前記第１の共通鍵に基づいて暗号化し、前記第２のインタフェース部に出力するための第１の暗号化処理部（１４０６）と、

前記第２の共通鍵によって暗号化され、さらに第２の公開暗号化鍵によって暗号化された、前記第２のライセンスデータ暗号化処理部からの前記ライセンスキーを受け、前記第２の共通鍵に基づいて復号するための第２の復号処理部（１４１０）と、

前記第２の公開暗号化鍵によって暗号化されたデータを復号するためのデータ格納部ごとに固有な第２の秘密復号鍵を保持する第３の鍵保持部（１４１５）と、

前記第２の公開暗号化鍵によって暗号化された前記ライセンスキーを受け、前記第２の秘密復号鍵により前記ライセンスキーを復号し抽出するための第３の復号処理部（１４１６）と、

前記暗号化コンテンツデータと前記ライセンスキーを格納するための記憶部（１４１２）とを備える、データ配信システム。

２．（補正後）各前記端末は、コンテンツ再生部をさらに備え、

前記コンテンツ再生部は、

第３の公開暗号化鍵にて暗号化されたデータを復号する第３の秘密復号鍵を保持するための第４の鍵保持部（１５２０）と、

前記データ格納部にて前記第３の公開暗号化鍵によって暗号化された前記第２の共通鍵を復号し抽出するための第４の復号処理部（１５２２）と、

第３の共通鍵を生成する第３のセッションキー発生部（１５０２）と、

前記第４の復号処理部にて復号し抽出した前記第２の共通鍵に基づいて、前記第３の共通鍵を暗号化し出力するための第２の暗号化処理部（１５０４）と、

前記データ格納部にて前記第３の共通鍵に基づいて暗号化された前記ライセン

スキーを復号し抽出するための第５の復号処理部（１５０６）と、

前記データ格納部から前記記憶部に記録された前記暗号化コンテンツデータの供給を受け、抽出した前記ライセンスキーにて復号し、再生するためのデータ再生部（１５０８）とをさらに備え、

前記データ格納部は、

前記第２のセッションキー発生部にて生成した前記第２の共通鍵を前記第３の公開暗号化鍵に基づいて暗号化する第３の暗号化処理部（１４３０）をさらに備え、

前記データ格納部は、前記コンテンツ再生部にて前記第２の共通鍵にて暗号化された前記第３の共通鍵を受けて、前記第２の復号処理部（１４１０）にて前記第２の共通鍵に基づいて復号し抽出した前記第３の共通鍵により、前記記憶部に格納された前記ライセンスキーを、前記第１の暗号化処理部にて暗号化し、前記コンテンツ再生部へ出力することを指示する、請求項１記載のデータ配信システム。

３．（補正後）前記データ格納部は、

他のデータ格納部に対して少なくとも前記ライセンスキーを移転するための移動処理において、前記他のデータ格納部の前記第１の公開暗号化鍵によって前記第２の共通鍵を暗号化するための第３の暗号化処理部（１４３０）と、

前記他のデータ格納部の第２の公開暗号化鍵による暗号化処理を行なうための第４の暗号化処理部（１４１４）とをさらに含み、

前記第２のセッションキー発生部は、前記移動処理に応じて、前記第２の共通鍵を発生し、

前記第２の暗号化処理部は、前記移動処理に応じて、前記他のデータ格納部から前記第２の共通鍵によって暗号化され、入力される第４の共通鍵と前記他のデータ格納部の第２の公開暗号化鍵とを復号して抽出し、

前記第４の暗号化処理部は、前記移動処理に応じて、前記他のデータ格納部の第２の公開暗号化鍵により、前記記憶部に格納された前記ライセンスキーを暗号化し、

前記第１の暗号化処理部は、前記移動処理に応じて、前記第４の暗号化処理部

の出力を前記第４の共通鍵にて暗号化し、前記他のデータ格納部に対して出力する、請求項１記載のデータ配信システム。

４．（補正後）前記他のデータ格納部の移動処理に応じて、前記データ格納部が前記他のデータ格納部から前記ライセンスキーの移転を受ける移動受理処理において、

前記第１の復号処理部は、前記移動受理処理において、前記第１の公開暗号化鍵によって暗号化され、入力される前記他のデータ格納部にて発生された前記第２の共通鍵を復号して抽出し、

前記第２のセッションキー発生部は、前記移動受理処理に応じて、前記第４の共通鍵を発生し、

前記第１の暗号化処理部は、前記移動受理処理に応じて、第２の共通鍵により、前記第２の公開暗号化鍵と前記第４の共通鍵とを暗号化して出力し、

前記第２の復号処理部は、前記他のデータ格納部において前記第２の公開暗号化鍵にて暗号化され、さらに前記第４の共通鍵にて暗号化されたライセンスキーを前記第４の共通鍵にて復号する、請求項３記載のデータ配信システム。

５．（補正後）前記記憶部は、前記第２の復号処理部の出力を受けて、前記第２の公開暗号化鍵により暗号化されている前記ライセンスキーを格納し、

前記第３の復号処理部は、前記記憶部に格納されている前記第２の公開暗号化鍵により暗号化されている前記ライセンスキーを、前記第２の秘密復号鍵にて復号する、請求項１記載のデータ配信システム。

６．（補正後）前記第３の復号処理部は、前記第２の復号処理部の出力を受けて、前記第２の公開暗号化鍵により暗号化されている前記ライセンスキーを、前記第２の秘密復号鍵にて復号し、

前記記憶部は、前記第３の復号処理部の出力を受けて、前記ライセンスキーを格納する、請求項１記載のデータ配信システム。

７．（補正後）暗号化コンテンツデータと前記暗号化データを復号するためのライセンスキーとのうち少なくとも前記ライセンスキーを、少なくとも前記ライセンスキーを格納可能なデータ格納部を備える複数のユーザの各端末に供給するためのデータ供給装置であって、

外部との間でデータを授受するためのインタフェース部（３５０）と、

前記ライセンスキーの通信ごとに更新される第１の共通鍵を生成するセッションキー発生部（３１４）と、

前記ユーザ端末の前記データ格納部に対応して予め定められた第１の公開暗号化鍵により前記第１の共通鍵を暗号化して前記インタフェース部に与えるためのセッションキー暗号化処理部（３１６）と、

前記第１の共通鍵により暗号化されて返信される第２の共通鍵と第２の公開暗号化鍵を復号し抽出するセッションキー復号部（３１８）と、

前記暗号化コンテンツデータを復号するための前記ライセンスキーを、前記セッションキー復号部により復号された前記第２の公開暗号化鍵により暗号化するための第１のライセンスデータ暗号化処理部（３２０）と、

前記第１のライセンスデータ暗号化処理部の出力を前記第２の共通鍵でさらに暗号化して前記インタフェース部に与え、各前記端末に供給するための第２のライセンス暗号化処理部（３２２）とを備える、データ供給装置。

８．（補正後）前記第１の公開暗号化鍵は、前記インタフェース部を介して各前記端末から与えられ、

前記セッションキー暗号化処理部は、前記与えられた第１の公開暗号化鍵により、前記第１の共通鍵を暗号化する、請求項７記載のデータ供給装置。

９．（補正後）前記データ供給装置は、

認証鍵を保持する認証鍵保持部と、

前記認証鍵により復号でき、かつ前記インタフェース部を介して各前記端末から取得する各前記端末の前記データ格納部に予め定められた認証データを復号して抽出するための認証復号処理部（３２６）と、

前記認証復号処理部により抽出された前記認証データに基づいて認証処理を行ない、前記認証データを取得した端末に対して少なくともライセンスキーを供給するか否かを判断する制御部（３１２）をさらに含む、請求項７記載のデータ供給装置。

１０．（補正後）前記第１の公開暗号化鍵は、前記認証データとともに前記認証鍵により復号できるように暗号化され、前記インタフェース部を介して各前記端

末から取得され、

前記認証データ復号処理部は、前記インタフェース部を介して取得された前記認証鍵により復号できるように暗号化された前記認証データと前記第１の公開暗号化鍵とを前記認証鍵にて復号して、前記認証データと前記第１の公開暗号化鍵とを抽出し、抽出した前記認証データを前記制御部に、抽出した前記第１の公開暗号化鍵を前記セッションキー暗号化処理部に出力する、請求項９記載のデータ供給装置。

１１．（補正後）前記データ供給装置は、

各前記端末にて復号可能な暗号化を行なうための端末共通暗号化鍵を保持する暗号化鍵保持部と、

前記暗号化鍵保持部に保持された前記端末共通暗号化鍵にて、前記ライセンスキーを暗号化し前記第１のライセンス暗号化処理部に対して出力する第３のライセンス暗号化処理部をさらに含む、請求項７記載のデータ供給装置。

１２．（補正後）暗号化コンテンツデータと前記暗号化コンテンツデータを復号するためのライセンスキーとのうち少なくとも前記ライセンスキーを複数の記録装置に供給するためのデータ供給装置であって、

前記記録装置との間でデータを授受するためのインタフェース部（３５０）と、

前記インタフェース部と前記記録装置を接続してデータを供給可能な接続部（２０１０、２０３０）と、

前記ライセンスキーの供給ごとに更新される第１の共通鍵を生成する第１のセッションキー発生部（３１４）と、

前記記録装置に対して予め定められた第１の公開暗号化鍵により前記第１の共通鍵を暗号化して前記インタフェース部に与えるためのセッションキー暗号化処理部（３１６）と、

前記第１の共通鍵により暗号化されて前記接続部に接続された記録装置より入力される第２の共通鍵と第２の公開暗号化鍵を復号し抽出するセッションキー復号部（３１８）と、

前記暗号化コンテンツデータを復号するためのライセンスキーを、前記セッションキー復号部により復号された前記第２の公開暗号化鍵により暗号化するため

の第１のライセンスデータ暗号化処理部（３２０）と

前記第１のライセンスデータ暗号化処理部の出力を前記第２の共通鍵でさらに暗号化して前記インタフェース部に与え、前記接続部に接続された記録装置に供給するための第２のライセンス暗号化処理部（３２２）とを備える、データ供給装置。

１３．（補正後）各前記記録装置は、メモリカードであって、

前記記録装置は、前記メモリカードと直接接続可能である、請求項１２記載のデータ供給装置。

１４．（補正後）前記第１の公開暗号化鍵は、前記インタフェース部を介して各前記記録装置から与えられ、

前記セッションキー暗号化処理部は、前記与えられた第１の公開暗号化鍵により前記第１の共通鍵を暗号化する、請求項１２記載のデータ供給装置。

１５．（補正後）前記データ供給装置は、

認証鍵により復号でき、かつ前記インタフェース部を介して各前記記録装置から与えられる認証データを復号して抽出するための認証復号処理部（３２６）と、

前記認証復号処理部により抽出された前記認証データに基づいて認証処理を行ない、少なくともライセンスキーを前記記録装置に対して出力するか否かを判断する制御部（３１２）をさらに含む、請求項１２記載のデータ供給装置。

１６．（補正後）前記第１の公開暗号化鍵は、前記認証データとともに前記認証鍵により復号できるように暗号化され、前記インタフェース部を介して各前記記録装置から取得され、

前記認証データ復号処理部は、前記インタフェース部を介して取得された前記認証鍵により復号できるように暗号化された前記認証データと前記第１の公開暗号化鍵を前記認証鍵にて復号して、前記認証データと前記第１の公開暗号化鍵とを抽出し、抽出した前記認証データを前記制御部に、抽出した前記第１の公開暗号化鍵を前記セッションキー暗号化処理部に出力する、請求項１５記載のデータ供給装置。

１７．（補正後）前記データ供給装置は、

各前記記録装置を装着して、前記記録装置に格納された前記ライセンスキーと

前記暗号化コンテンツデータを取得して、前記暗号化コンテンツデータからコンテンツデータを復号する複数の端末にて復号可能な暗号化を行なうための端末共通暗号化鍵を保持する暗号化鍵保持部（３３０）と、

前記暗号化鍵保持部に保持された前記端末共通暗号化鍵に基づいて、前記ライセンスキーを暗号化し、前記第１のライセンス暗号化処理部に対して出力する第３のライセンス暗号化処理部（３３２）とをさらに含む、請求項１０に記載のデータ供給装置。

１８．（補正後）前記記録装置は、前記インタフェース部と接続して外部からデータを受ける端子数を切換え、１ビットごとのデータ通信を行なうシリアルモードと、複数のビットごとのデータ通信を行なうパラレルモードとを切換えるための手段を備え、

前記データ供給装置は、

前記インタフェース部を介して、前記記録装置に対して、前記ライセンスキーとともに前記暗号化コンテンツデータを供給し、

前記インタフェース部は、

少なくとも前記暗号化コンテンツデータを、前記記録装置に入力する場合に、前記記録装置に対してパラレルモードを指示する、請求項１２記載のデータ供給装置。

１９．（補正後）データ供給装置から、暗号化コンテンツデータと前記暗号化コンテンツデータを復号するためのライセンスキーとのうち少なくとも前記ライセンスキーの配信を受けるための端末装置であって、

外部との間にデータを授受するための第１のインタフェース部と、

前記ライセンスキーを受けて格納するデータ格納部（１４０）とを備え、

前記データ格納部は、

第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の鍵保持部（１４０２）と、

前記第１の公開暗号化鍵によって暗号化され外部から入力された第１の共通鍵を受けて、復号処理するための第１の復号処理部（１４０４）と、

前記データ格納部ごとに固有な第２の公開暗号化鍵を保持するための第２の鍵

保持部（１４０５）と、

第２の共通鍵を生成する第２のセッションキー発生部（１４３２）と、

前記第２の公開暗号化鍵と前記第２の共通鍵を、前記第１の共通鍵に基づいて暗号化し、前記第１のインタフェース部に出力するための第１の暗号化処理部（１４０６）と、

前記第２の公開暗号化鍵によって暗号化され、さらに前記第２の共通鍵によって暗号化されたライセンスキーを受け、前記第２の共通鍵に基づいて復号するための第２の復号処理部（１４１０）と、

前記第２の公開暗号化鍵によって暗号化されたデータを復号化するための前記データ格納部ごとに固有な第２の秘密復号鍵を保持する第３の鍵保持部（１４１５）と、

前記第２の復号処理部の出力を受けて、前記第２の公開暗号化鍵によって暗号化された前記ライセンスキーを格納するための記憶部（１４１２）と、

前記記憶部に格納された第２の公開暗号化鍵によって暗号化されたライセンスキーを受け、前記第２の秘密復号鍵により復号するための第３の復号処理部（１４１６）とを備える、端末装置。

２０．（補正後）前記データ格納部は、前記端末装置に着脱可能な記録装置である、請求項１９記載の端末装置。

２１．（補正後）前記データ格納部は、

前記第１の公開暗号化鍵を保持し、外部に出力可能な第４の鍵保持部（１４０１）をさらに含む、請求項１９記載の端末装置。

２２．（補正後）前記データ格納部は、

前記第１の公開暗号化鍵と、前記データ格納部に固有で、かつ、第１の公開暗号化鍵に対して一意に定められた第１の認証データとを、予め定められた認証鍵により復号できるように暗号化して保持する第１のデータ保持部（１４４２）をさらに含む、請求項１９記載の端末装置。

２３．（補正後）前記端末装置は、コンテンツ再生部をさらに備え、

前記コンテンツ再生部は、

前記コンテンツ再生部に固有な第３の公開暗号化鍵によって暗号化されたデー

タを復号する第[redacted]秘密復号鍵を保持するための第[redacted]鍵保持部（１５２０）と、

前記データ格納部にて前記第３の公開暗号化鍵によって暗号化された前記第２の共通鍵を復号し抽出するための第４の復号処理部（１５２２）と、

第３の共通鍵を生成する第３のセッションキー発生部（１５０２）と、

前記第４の復号処理部にて復号し抽出した前記第２の共通鍵に基づいて、前記第３の共通鍵を暗号化し出力するための第２の暗号化処理部（１５０４）と、

前記データ格納部にて前記第３の共通鍵に基づいて暗号化されたライセンスキーを復号し抽出するための第５の復号処理部（１５０６）と、

前記記憶部に記録された暗号化コンテンツデータを、抽出した前記ライセンスキーにて復号し、再生するためのデータ再生部（１５０８）とをさらに備え、

前記データ格納部は、

前記第２のセッションキー発生部にて生成した前記第２の共通鍵を前記第３の公開暗号化鍵に基づいて暗号化する第３の暗号化処理部（１４３０）をさらに含み、

前記第２の復号処理部（１４１０）は、さらに、前記コンテンツ再生部にて前記第２の共通鍵にて暗号化された前記第３の共通鍵を受けて、前記第２の共通鍵に基づいて復号して、前記第３の共通鍵を抽出し、

前記第３の復号処理部は、前記記憶部に格納されている前記第２の公開暗号化鍵により暗号化されている前記ライセンスキーを前記第２の秘密復号鍵に基づいて復号して、前記ライセンスキーを抽出し、

前記第１の暗号化処理部は、さらに、前記第２の復号処理部にて抽出した前記第３の共通鍵に基づいて、前記第３の復号処理部にて抽出された前記ライセンスキーを暗号化して前記コンテンツ再生部に与える、請求項１９記載の端末装置。

２４．（補正後）前記コンテンツ再生部は、

前記第３の公開暗号化鍵を保持し、外部に出力可能な第６の鍵保持部（１５２４）をさらに備える、請求項２３記載の端末装置。

２５．（補正後）前記コンテンツ再生部は、

前記第３の公開暗号化鍵と、前記データ格納部に固有で、かつ、第３の公開暗号化鍵にて一意に定められた第２の認証データとを、予め定められた認証鍵によ

り復号できるよ[redacted]暗号化して保持する第２のデー[redacted]持部（１５２５）をさらに含み、

前記データ格納部は、

前記認証鍵を保持する認証鍵保持部と、

前記データ格納部から入力された前記第２の認証データを、前記認証鍵に基づいて復号し、前記第３の公開暗号化鍵と前記第１の認証データとを抽出する認証データ復号処理部と、

前記第２の認証データに基づいて認証処理を行ない、少なくともライセンスキーを前記コンテンツ再生部に対して出力するか否かを判断する制御部（１４２０）をさらに含み、

前記認証データ復号処理部は、抽出した前記第３の公開暗号化鍵前記を第３の暗号化処理部に、抽出した前記第２の認証データを前記制御部に対して出力する、請求項２３記載の端末装置。

２６．（補正後）前記ライセンスキーは複数の各前記端末装置にて共通な端末共通復号鍵にて復号可能な暗号化を施して記憶部に格納され、

前記コンテンツ再生部は、

前記端末共通復号鍵を保持する復号鍵保持部と、

前記第５の復号処理部からの出力を前記端末共通復号鍵に基づいて復号し、前記ライセンスキーを抽出する第６の復号処理部とをさらに含む、請求項２３記載の端末装置。

２７．（補正後）前記データ格納部は、

他のデータ格納部に対して少なくとも前記ライセンスキーを移転するための移動処理に応じて、前記他のデータ格納部の前記第１の公開暗号化鍵によって前記第２の共通鍵を暗号化するための第３の暗号化処理部（１４３０）と、

前記他のデータ格納部の第２の公開暗号化鍵による暗号化処理を行なうための第４の暗号化処理部（１４１４）とをさらに含み、

前記第２のセッションキー発生部は、前記移動処理に応じて、前記第２の共通鍵を発生し、

前記第２の復号処理部は、前記移動処理に応じて、前記他のデータ格納部から

前記第２の共通[redacted]よって暗号化され、入力される[redacted]の共通鍵と前記他のデータ格納部の第２の公開暗号化鍵とを復号して抽出し、

前記第３の復号処理部は、前記移動処理に応じて、前記第２の秘密復号鍵に基づいて、前記記憶部に格納された前記第２の公開暗号化鍵にて暗号化されたデータを復号して前記ライセンスキーを抽出し、

前記第４の暗号化処理部は、前記移動処理に応じて、前記他のデータ格納部の第２の公開暗号化鍵に基づいて、抽出された前記ライセンスキーを暗号化し、

前記第１の暗号化処理部は、前記移動処理に応じて、抽出した前記第４の共通鍵にて前記第４の暗号化処理部の出力を暗号化し、前記他のデータ格納部に対して出力する、請求項１９記載の端末装置。

２８．（補正後）前記データ格納部は、

他のデータ格納部に対して少なくとも前記ライセンスキーを移転するための移動処理に応じて、前記他のデータ格納部から出力される前記第１の公開暗号化鍵によって前記第２の共通鍵を暗号化するための第３の暗号化処理部（１４３０）と、

前記他のデータ格納部の第２の公開暗号化鍵による暗号化処理を行なうための第４の暗号化処理部（１４１４）とをさらに含み、

前記第２のセッションキー発生部は、前記移動処理に応じて、前記第２の共通鍵を発生し、

前記第２の復号処理部は、前記移動処理に応じて、前記他のデータ格納部から前記第２の共通鍵によって暗号化され、入力される第４の共通鍵と前記他のデータ格納部の第２の公開暗号化鍵とを復号して抽出し、

前記第３の復号処理部は、前記移動処理に応じて、前記第２の秘密復号鍵に基づいて、前記記憶部に格納された前記第２の公開暗号化鍵にて暗号化されたデータを復号して前記ライセンスキーを抽出し、

前記第４の暗号化処理部は、前記移動処理に応じて、前記他のデータ格納部の第２の公開暗号化鍵に基づいて、抽出された前記ライセンスキーを暗号化し、

前記第１の暗号化処理部は、前記移動処理に応じて、前記第４の暗号化処理部の出力を抽出した前記第４の共通鍵にて暗号化し、前記他のデータ格納部に対し

て出力する、請求項２１記載の端末装置。

２９．（補正後）前記データ格納部は、

前記認証鍵を保持する認証鍵保持部と、

他のデータ格納部に対して少なくとも前記ライセンスキーを移転するための移動処理に応じて、前記他のデータ格納部から入力された前記第１の認証データを、前記認証鍵に基づいて復号し、前記第１の公開暗号化鍵と前記第１の認証データとを抽出する認証データ復号処理部と、

前記移動処理に応じて、前記第１の認証データに基づいて認証処理を行ない、少なくともライセンスキーを前記他のデータ格納部に対して出力するか否かを判断する制御部（１４２０）と、

前記移動処理に応じて、前記他のデータ格納部から出力される前記第１の公開暗号化鍵によって前記第２の共通鍵を暗号化するための第３の暗号化処理部（１４３０）と、

前記他のデータ格納部の第２の公開暗号化鍵による暗号化処理を行なうための第４の暗号化処理部（１４１４）とをさらに含み、

前記第２のセッションキー発生部は、前記移動処理に応じて、前記第２の共通鍵を発生し、

前記第２の復号処理部は、前記移動処理に応じて、前記他のデータ格納部から前記第２の共通鍵によって暗号化され、入力される第４の共通鍵と前記他のデータ格納部の第２の公開暗号化鍵とを復号して抽出し、

前記第３の復号処理部は、前記移動処理に応じて、前記第２の秘密復号鍵に基づいて、前記記憶部に格納された前記第２の公開暗号化鍵にて暗号化されたデータを復号してライセンスキーを抽出し、

前記第４の暗号化処理部は、前記移動処理に応じて、前記他のデータ格納部の第２の公開暗号化鍵に基づいて、抽出された前記ライセンスキーを暗号化し、

前記第１の暗号化処理部は、前記移動処理に応じて、前記第４の暗号化処理部の出力を抽出した前記第４の共通鍵にて暗号化し、前記他のデータ格納部に対して出力する、請求項２０に記載の端末装置。

３０．（補正後）データ供給装置から、暗号化コンテンツデータと前記暗号化コ

ンテンツデータを復号するためのライセンスキーとの少なくとも前記ライセンスキーの配信を受けるための端末装置であって、

外部との間にデータを授受するための第１のインタフェース部と、

前記ライセンスキーを受けて格納するデータ格納部（１４０）とを備え、

前記データ格納部は、

第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の鍵保持部（１４０２）と、

前記第１の公開暗号化鍵によって暗号化され外部から入力された第１の共通鍵を受けて、復号処理するための第１の復号処理部（１４０４）と、

前記データ格納部ごとに固有な第２の公開暗号化鍵を保持するための第２の鍵保持部（１４０５）と、

第２の共通鍵を生成する第２のセッションキー発生部（１４３２）と、

前記第２の公開暗号化鍵と前記第２の共通鍵を、前記第１の共通鍵に基づいて暗号化し、前記第１のインタフェース部に出力するための第１の暗号化処理部（１４０６）と、

前記第２の公開暗号化鍵にて暗号化され、さらに前記第２の共通鍵によって暗号化されたライセンスキーを受け、前記第２の共通鍵に基づいて復号するための第２の復号処理部（１４１０）と、

前記第２の公開暗号化鍵によって暗号化されたデータを復号するための前記データ格納部ごとに固有な第２の秘密復号鍵を保持する第３の鍵保持部（１４１５）と、

前記第２の公開暗号化鍵によって暗号化された前記ライセンスキーを受け、前記第２の秘密復号鍵により復号するための第３の復号処理部（１４１６）と、

前記第３の復号処理部の出力を受けて、前記ライセンスキーを格納するための記憶部（１４１２）とを備える、端末装置。

３１．（補正後）前記データ格納部は、前記端末装置に着脱可能な記録装置である、請求項３０記載の端末装置。

３２．（補正後）前記データ格納部は、

前記第１の公開暗号化鍵を保持し、外部に出力可能な第４の鍵保持部（１４０

1）をさらに含む、請求項３０記載の端末装置。

３３．（補正後）前記データ格納部は、

前記第１の公開暗号化鍵と、前記データ格納部に固有で、かつ、第１の公開暗号化鍵に対して一意に定められた第１の認証データとを、予め定められた認証鍵により復号できるように暗号化して保持する第１のデータ保持部（１４４２）をさらに含む、請求項３０記載の端末装置。

３４．（追加）前記端末装置は、コンテンツ再生部をさらに備え、

前記コンテンツ再生部は、

前記コンテンツ再生部に対して予め定められた第３の公開暗号化鍵によって暗号化されたデータを復号する第３の秘密復号鍵を保持するための第５の鍵保持部（１５２０）と、

前記データ格納部にて前記第３の公開暗号化鍵によって暗号化された前記第２の共通鍵を復号し抽出するための第４の復号処理部（１５２２）と、

第３の共通鍵を生成する第３のセッションキー発生部（１５０２）と、

前記第４の復号処理部にて復号し抽出した前記第２の共通鍵に基づいて、前記第３の共通鍵を暗号化し出力するための第２の暗号化処理部（１５０４）と、

前記データ格納部にて前記第３の共通鍵に基づいて暗号化されたライセンスキーを復号し抽出するための第５の復号処理部（１５０６）と、

前記記憶部に記録された暗号化コンテンツデータを、抽出した前記ライセンスキーにて復号し、再生するためのデータ再生部（１５０８）とをさらに含み、

前記データ格納部は、

前記第２のセッションキー発生部にて生成した前記第２の共通鍵を前記第３の公開暗号化鍵に基づいて暗号化する第３の暗号化処理部（１４３０）をさらに含み、

前記第２の復号処理部（１４１０）は、さらに、前記コンテンツ再生部にて前記第２の共通鍵にて暗号化された前記第３の共通鍵を受けて、前記第２の共通鍵に基づいて復号して前記第３の共通鍵を抽出し、

前記第１の暗号化処理部は、さらに、前記第２の復号処理部にて抽出した前記第３の共通鍵に基づいて、前記記憶部に格納されている前記ライセンスキーを暗

号化して前記コ[redacted]ンツ再生部に与える、請求項２[redacted]載の端末装置。

３５．（追加）前記コンテンツ再生部は、

前記第３の公開暗号化鍵を保持し、外部に出力可能な第６の鍵保持部（１５２４）をさらに含む、請求項３４記載の端末装置。

３６．（追加）前記コンテンツ再生部は、

前記第３の公開暗号化鍵と、前記データ格納部に固有で、かつ、第３の公開暗号化鍵に対して一意に定められた第２の認証データとを、予め定められた認証鍵により復号できるように暗号化して保持する第２のデータ保持部（１５２５）をさらに含み、

前記データ格納部は、

前記認証鍵を保持する認証鍵保持部と、

前記データ格納部から入力された前記第２の認証データを、前記認証鍵に基づいて復号し、前記第３の公開暗号化鍵と、前記第１の認証データとを抽出する認証データ復号処理部と、

前記第２の認証データに基づいて認証処理を行ない、少なくともライセンスキーを前記コンテンツ再生部に対して出力するか否かを判断する制御部（１４２０）とをさらに含み、

前記認証データ復号処理部は、抽出した第３の公開暗号化鍵を前記第３の暗号化処理部に、抽出した第２の認証データを前記制御部に対して出力する、請求項３４記載の端末装置。

３７．（追加）前記ライセンスキーは、複数の各前記端末装置にて共通な端末共通復号鍵にて復号可能な暗号化を施して記憶部に格納され、

前記コンテンツ再生部は、

前記端末共通復号鍵を保持する復号鍵保持部と、

前記第５の復号処理部からの出力を、前記端末共通復号鍵に基づいて復号し、前記ライセンスキーを抽出する第６の復号処理部とをさらに含む、請求項３４記載の端末装置。

３８．（追加）前記データ格納部は、

他のデータ格納部に対して少なくとも前記ライセンスキーを移転するための移

動処理に応じて、前記他のデータ格納部の前記第１の公開暗号化鍵によって前記第２の共通鍵を暗号化するための第３の暗号化処理部（１４３０）と、

前記他のデータ格納部の第２の公開暗号化鍵による暗号化処理を行なうための第４の暗号化処理部（１４１４）とをさらに含み、

前記第２のセッションキー発生部は、前記移動処理に応じて、前記第２の共通鍵を発生し、

前記第２の復号処理部は、前記移動処理に応じて、前記他のデータ格納部から前記第２の共通鍵によって暗号化され、入力される第４の共通鍵と前記他のデータ格納部の第２の公開暗号化鍵とを復号して抽出し、

前記第４の暗号化処理部は、前記移動処理に応じて、前記他のデータ格納部の第２の公開暗号化鍵に基づいて、前記記憶部に格納された前記ライセンスキーを暗号化し、

前記第１の暗号化処理部は、前記移動処理に応じて、前記第４の暗号化処理部の出力を抽出した前記第４の共通鍵にて暗号化し、前記他のデータ格納部に対して出力する、請求項３０記載の端末装置。

３９．（追加）前記データ格納部は、

前記第１の公開暗号化鍵を保持し、外部に出力可能な第４の鍵保持部（１４０１）をさらに含み、

前記第３の暗号化処理部は、前記移動処理に応じて、前記他のデータ格納部から入力された前記第１の公開暗号化鍵に基づいて暗号化する、請求項３８記載の端末装置。

４０．（追加）前記データ格納部は、

他のデータ格納部に対して少なくとも前記ライセンスキーを移転するための移動処理に応じて、前記他のデータ格納部から出力される前記第１の公開暗号化鍵によって前記第２の共通鍵を暗号化するための第３の暗号化処理部（１４３０）と、

前記他のデータ格納部の第２の公開暗号化鍵による暗号化処理を行なうための第４の暗号化処理部（１４１４）とをさらに含み、

前記第２のセッションキー発生部は、前記移動処理に応じて、前記第２の共通

鍵を発生し、

前記第２の復号処理部は、前記移動処理に応じて、前記他のデータ格納部から前記第２の共通鍵によって暗号化され、入力される第４の共通鍵と前記他のデータ格納部の第２の公開暗号化鍵とを復号して抽出し、

前記第３の復号処理部は、前記移動処理に応じて、前記第２の秘密復号鍵に基づいて、前記記憶部に格納された前記第２の公開暗号化鍵にて暗号化されたデータを復号して前記ライセンスキーを抽出し、

前記第４の暗号化処理部は、前記移動処理に応じて、前記他のデータ格納部の第２の公開暗号化鍵に基づいて抽出された前記ライセンスキーを暗号化し、

前記第１の暗号化処理部は、前記移動処理に応じて、前記第４の暗号化処理部の出力を抽出した前記第４の共通鍵にて暗号化し、前記他のデータ格納部に対して出力する、請求項３２記載の端末装置。

４１．（追加）前記データ格納部は、

前記認証鍵を保持する認証鍵保持部と、

他のデータ格納部に対して少なくとも前記ライセンスキーを移転するための移動処理に応じて、前記他のデータ格納部から入力された前記第１の認証データを、前記認証鍵に基づいて復号し、前記第１の公開暗号化鍵と前記第１の認証データとを抽出する認証データ復号処理部と、

前記移動処理に応じて、前記第１の認証データに基づいて認証処理を行ない、少なくともライセンスキーを前記他のデータ格納部に対して出力するか否かを判断する制御部（１４２０）と、

前記移動処理に応じて、前記他のデータ格納部から出力される前記第１の公開暗号化鍵によって前記第２の共通鍵を暗号化するための第３の暗号化処理部（１４３０）と、

前記他のデータ格納部の第２の公開暗号化鍵による暗号化処理を行なうための第４の暗号化処理部（１４１４）とをさらに含み、

前記第２のセッションキー発生部は、前記移動処理に応じて、前記第２の共通鍵を発生し、

前記第２の復号処理部は、前記移動処理に応じて、前記他のデータ格納部から

前記第２の共通鍵によって暗号化され、入力される第３の共通鍵と前記他のデータ格納部の第２の公開暗号化鍵とを復号して抽出し、

前記第３の復号処理部は、前記移動処理に応じて、前記第２の秘密復号鍵に基づいて、前記記憶部に格納された前記第２の公開暗号化鍵にて暗号化されたデータを復号してライセンスキーを抽出し、

前記第４の暗号化処理部は、前記移動処理に応じて、前記他のデータ格納部の第２の公開暗号化鍵に基づいて、抽出された前記ライセンスキーを暗号化し、

前記第１の暗号化処理部は、前記移動処理に応じて、前記第４の暗号化処理部の出力を抽出した前記第４の共通鍵にて暗号化し、前記他のデータ格納部に対して出力する、請求項３３記載の端末装置。

４２．（追加）データ供給装置から暗号化コンテンツデータと前記暗号化コンテンツデータを復号するためのライセンスキーとのうち少なくとも前記ライセンスキーの配信を受けるための端末装置であって、

前記データ供給装置との間でデータを授受するための第１のインタフェース部と、

コンテンツ再生部と、

前記端末装置に着脱可能なデータ格納部と接続するための第２のインタフェース部とを備え、

前記コンテンツ再生部は、

第３の公開暗号化鍵にて暗号化されるデータを復号する第３の秘密復号鍵を保持するための第４の鍵保持部（１５２０）と、

前記データ格納部にて前記第３の公開暗号化鍵によって暗号化された前記第２の共通鍵を復号し抽出するための第４の復号処理部（１５２２）と、

第３の共通鍵を生成する第３のセッションキー発生部（１５０２）と、

前記第４の復号処理部にて復号し抽出した前記第２の共通鍵に基づいて、前記第３の共通鍵を暗号化し出力するための第２の暗号化処理部（１５０４）と、

前記データ格納部にて前記第３の共通鍵に基づいて暗号化されたライセンスキーを復号し抽出するための第５の復号処理部（１５０６）と、

前記データ格納部に記録された暗号化コンテンツデータを、抽出したライセン

スキーにて復号[redacted]再生するためのデータ再生部（1[redacted]０８）とを含む、端末装置。

４３．認証鍵により復号できるように、第２の認証データと前記第３の公開暗号化鍵とを保持し、外部に出力するためのデータ保持部（１５２５）をさらに含む、請求項４２記載の端末装置。

４４．（補正後）暗号化コンテンツデータと前記暗号化コンテンツデータを復号するためのライセンスキーとを格納するための記録装置であって、

外部との間でデータ授受を行なうためのインタフェース部と、

データを記録する記録部（１４１２）と、

前記インタフェース部と前記記録部間のデータの伝達を行うｍビット幅（ｍは自然数、ｍ＞１）のパラレルデータバス（ＢＳ３）とを備え、

前記インタフェース部は、

複数の端子（１４６２．０－１４６２．３）と、

外部からの入力データのビット幅の切換指令に従って、外部からデータを受ける端子として前記複数の端子から１個またはｎ個（ｎは自然数、１＜ｎ≦ｍ）の予め定められた端子を選択する選択手段と、

前記切換指令に応じて、選択された前記１個の端子を介して外部から与えられたシリアルデータ、または前記ｎ個の端子を介して、外部から与えられたｎビット幅のパラレルデータをｍビット幅のパラレルデータに変換し、前記パラレルデータバスへ供給する第１の変換手段と、

前記パラレルデータバスからのｍビット幅のパラレルデータをシリアルデータに変換して、前記複数の端子の予め定められた１個の端子を介して外部へ出力する第２の変換手段とを含み、

第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の鍵保持部（１４０２）と、

前記第１の公開暗号化鍵によって暗号化された第１の共通鍵を受けて、前記第１の秘密復号鍵に基づいて復号処理するための第１の復号処理部（１４０４）と、

第２の公開暗号化鍵を保持するための第２の鍵保持部（１４０５）と、

第２の共通鍵を生成するセッションキー発生部（１４３２）と、

前記第２の公[redacted]号化鍵と前記第２の共通鍵を前記[redacted]１の共通鍵に基づいて暗号化し、前記パラレルデータバスを介して前記インタフェース部に出力するための第１の暗号化処理部（１４０６）と、

前記第２の公開暗号化鍵で暗号化され、さらに前記第２の共通鍵にて暗号化されたライセンスキーを受け、前記第２の共通鍵に基づいて復号するための第２の復号処理部（１４１０）と、

前記第２の公開暗号化鍵によって暗号化されたデータを復号化するための前記記録装置ごとに設定された第２の秘密復号鍵を保持する第３の鍵保持部（１４１５）と、

前記第２の公開暗号化鍵で暗号化されたライセンスキーを受けて、前記第２の秘密復号鍵に基づいて復号して、前記ライセンスキーを抽出する第３の復号処理部（１４１６）とをさらに備え、

前記記録部は、前記暗号化コンテンツデータと前記ライセンスキーを格納する、記録装置。

４５．（補正後）外部に出力するために、前記第１の公開暗号化鍵と前記第１の公開暗号化鍵と対応する証明データとを、外部にて認証鍵にて復号できるように暗号化した認証データを保持するための認証データ保持部（１４４２）をさらに備える、請求項４４記載の記録装置。

４６．（削除）

補正された用紙(条約第34条)

CLAIMS

1. A data distribution system for distributing encrypted content data to each of terminals of a plurality of users from a content data supply device, comprising:

a first interface unit (350) for externally transmitting data;

a first session key generating unit (314) for producing a first symmetric key to be updated in response to every transmission of said encrypted content data;

a session key encryption processing unit (316) for encrypting said first symmetric key with a first public encryption key predetermined corresponding to said user's terminal, and applying the encrypted first symmetric key to said first interface unit;

a session key decrypting unit (318) for decrypting returned data encrypted with said first symmetric key;

a first license data encryption processing unit (320) for encrypting a license key for decrypting said encrypted content data using, as key data, the data decrypted by said session key decrypting unit; and

a second license data encryption processing unit (322) for further encrypting an output of said first license data encryption processing unit with a second symmetric key, and applying the encrypted output to said first interface unit for distribution, wherein

each of said terminals (100) includes:

a second interface unit for externally transmitting the data, and

a distributed data decoding unit (110) for receiving and storing said encrypted content data; and

said distributed data decoding unit includes:

a first key holding unit (1402) for holding a first private decryption key for decrypting the data encrypted by said first public encryption key,

a first decryption processing unit (1404) for receiving and decrypting said first symmetric key encrypted with said first public encryption key,

a second key holding unit (1405) for holding a second public encryption key,

a first encryption processing unit (1406) for encrypting said second public encryption key based on said first symmetric key, and outputting the encrypted second public encryption key to said second interface unit,

a second decryption processing unit (1410) for receiving the license key encrypted by said second license data encryption processing unit, and decrypting the received license key based on said second symmetric key,

a first memory unit (1412) for storing said encrypted content data allowing decryption based on said license key,

a third key holding unit (1415) for holding a second private decryption key for decrypting the data encrypted with said second public encryption key, and

a third decryption processing unit (1416) for decrypting said license key with said second private decryption key based on a result of the decryption by said second decryption processing unit.

2. The data distribution system according to claim 1, wherein

said distributed data decoding unit is a memory card releasably attached to said terminal,

said first private decryption key is predetermined depending on the type of said memory card, and

said second private decryption key is unique to each of said memory cards.

3. The data distribution system according to claim 1, wherein

said first private decryption key is predetermined in advance depending on a type of said distributed data decoding unit, and

said second private decryption key is unique to said distributed data decoding unit.

4. The data distribution system according to claim 2, wherein

said second and third decryption processing units receive license information data encrypted by said content data supply device with said second public encryption key, further decrypted with said second symmetric

key and distributed together with said license key via said second interface unit, and decrypts the received license information data with said second symmetric key and said second private decryption key; and

said distributed data decoding unit further includes a second memory unit (1500) for storing said decrypted license information data.

5. The data distribution system according to claim 4, wherein

said second memory unit further stores said license key decrypted by said third decryption processing unit.

6. The data distribution system according to claim 4, wherein

said first symmetric key and said second symmetric key have the same key data produced by said first session key generating unit at the time of communication of said encrypted content data.

7. The data distribution system according to claim 6, wherein

said distributed data decoding unit further includes a control unit for determining reproducibility based on the license information data stored in said second memory unit in response to the externally instructed reproducing operation mode, and controlling the operations of said distributed data decoding unit;

said first encryption processing unit is controlled by said control unit to receive said license key from said third decryption processing unit in response to the instruction of the reproducing operation of said content data, and encrypt the received license key with a third symmetric key for output;

said first memory unit is controlled by said control unit to output said encrypted content data in response to the instruction of the reproducing operation of said content data; and

each of said terminals further includes:

a second session key generating unit (1502) for producing said third symmetric key to be updated in response to every transmission of said encrypted content data, and

a content data reproducing unit (1506, 1508) operating to receive, decrypt and extract said license key encrypted with said third symmetric key applied from said distributed data encrypting unit, and operating to decrypt and reproduce said encrypted content data output from said first memory unit with said license key.

8. The data distribution system according to claim 7, wherein said distributed data decoding unit includes:

a control unit (1420) for controlling an operation of said distributed data decoding unit in accordance with a transfer operation mode for transferring said encrypted content data and said license information data to externally designated another terminal, and

a second encryption processing unit (1414) for performing encryption with a third public encryption key;

said second decryption processing unit is controlled by said control unit to decrypt and extract said third public encryption key encrypted with said third symmetric key and sent from the side of said externally designated terminal in response to the designation of said transfer operation mode;

said second encryption processing unit encrypts said license key and said license information data with said third public encryption key in response to the designation of said transfer operation mode;

said first encryption processing unit receives and encrypts the output of said second encryption processing unit based on said third symmetric key for applying the encrypted output to said second interface unit;

said control unit erases said license information data stored in said second memory unit in response to designation of said transfer operation mode; and

said first memory unit applies said encrypted content data to said second interface unit in response to designation of said transfer operation mode.

9. The data distribution system according to claim 7, wherein

said distributed data decoding unit further includes a control unit for controlling said distributed data decoding unit in response to a duplication operation mode for transferring said encrypted content data to externally designated another terminal, and

said first memory unit applies said encrypted content data to said second interface unit in response to designation of said duplication operation mode.

10. The data distribution system according to claim 4, wherein said distributed data decoding unit further includes:

a third session key generating unit (1432) for producing said second symmetric key, and

a third encryption processing unit (1430) for encrypting and applying the output of said third session key generating unit to said second interface unit.

11. The data distribution system according to claim 10, wherein

said distributed data decoding unit further includes a control unit for determining reproducibility based on the license information data stored in said second memory unit in response to the externally instructed reproducing operation mode, and controlling the operations of said distributed data decoding unit;

said third encryption processing unit encrypts the output of said third session key generating unit with a fourth public encryption key, and output the encrypted output to said second interface unit;

said first encryption processing unit is controlled by said control unit to receive said license key from said third decryption processing unit in response to the instruction of the reproducing operation of said content data, and encrypt the received license key with a third symmetric key for output;

said first memory unit is controlled by said control unit to output said encrypted content data in response to the instruction of the reproducing operation of said content data; and

each of said terminals further includes:

a second session key generating unit (1502) for producing said third symmetric key to be updated in response to every transmission of said encrypted content data,

a public key holding unit (1524) for applying said fourth public encryption key to said distributed data decoding unit,

a public key decrypting unit (1522) for decrypting said second symmetric key decrypted with said fourth public encryption key, and

a content data reproducing unit (1506, 1508) operating to receive, decrypt and extract said license key encrypted with said third symmetric key applied from said distributed data encrypting unit, and operating to decrypt and reproduce said encrypted content data output from said first memory unit with said license key.

12. The data distribution system according to claim 11, wherein said distributed data decoding unit includes:

a control unit for controlling an operation of said distributed data decoding unit in accordance with a transfer operation mode for transferring said encrypted content data and said license information data to externally designated another terminal, and

a second encryption processing unit for performing encryption with a third public encryption key;

said second decryption processing unit is controlled by said control unit to decrypt and extract said third public encryption key encrypted with said third symmetric key and sent from the side of said externally designated terminal in response to the designation of said transfer operation mode;

said second encryption processing unit encrypts said license key and said license information data with said third public encryption key in response to the designation of said transfer operation mode;

said first encryption processing unit receives and encrypts the output of said second encryption processing unit based on said third symmetric key for applying the encrypted output to said second interface unit;

said control unit erases said license information data stored in said second memory unit in response to designation of said transfer operation mode; and

said first memory unit applies said encrypted content data to said second interface unit in response to designation of said transfer operation mode.

13. The data distribution system according to claim 11, wherein

said distributed data decoding unit further includes a control unit for controlling said distributed data decoding unit in response to a duplication operation mode for transferring said encrypted content data to externally designated another terminal, and

said first memory unit applies said encrypted content data to said second interface unit in response to designation of said duplication operation mode.

14. The data distribution system according to claim 1, wherein

said first and second interface units are connected together over a cellular phone network, and

said content data supply device authenticates said user based on said first public encryption key.

15. The data distribution system according to claim 1, wherein

said first interface unit includes a connecting unit (2010) directly connectable to said terminal.

16. The data distribution system according to claim 2, wherein

said first interface unit includes a connecting unit (2030) directly connectable to said memory card.

17. A data distribution system for distributing at least one of encrypted data and a license key for decrypting said encrypted content data from a content data supply device to each of terminals of a plurality of

~~users, comprising:~~

a first interface unit (350) for externally transmitting data;

a first session key generating unit (314) for producing a first symmetric key to be updated in response to every transmission of said encrypted content data;

a session key encryption processing unit (316) for encrypting said first symmetric key with a first public encryption key predetermined corresponding to said user's terminal, and applying the encrypted first symmetric key to said first interface unit;

a session key decrypting unit (318) for decrypting and extracting a second symmetric key and a second public encryption key both encrypted with said first symmetric key and returned;

a first license data encryption processing unit (320) for encrypting a license key for decrypting said encrypted content data with said second public encryption key decrypted by said session key decrypting unit; and

a second license data encryption processing unit (322) for further encrypting an output of said first license data encryption processing unit with said second symmetric key, and applying the encrypted output to said first interface unit for distribution, wherein

each of said terminals includes:

a second interface unit for externally transmitting the data, and

a distributed data decoding unit (140) for receiving and storing said encrypted content data and said license key;

said distributed data decoding unit includes:

a first key holding unit (1402) for holding a first private decryption key for decrypting the data encrypted by said first public encryption key,

a first decryption processing unit (1404) for receiving and decrypting said first symmetric key encrypted with said first public encryption key,

a second key holding unit (1405) for holding a second public encryption key,

a second session key generating unit (1432) for producing said second symmetric key,

a first encryption processing unit (1406) for encrypting said second

public encryption key and said second symmetric key based on said first symmetric key, and outputting the encrypted keys to said second interface unit,

a second decryption processing unit (1410) for receiving the license key encrypted by said second license data encryption processing unit, and decrypting the received license key based on said second symmetric key,

a memory unit for storing said encrypted content data allowing decryption with said license key,

a third key holding unit (1415) for holding a second private decryption key for decrypting the data encrypted with said second public encryption key,

a third decryption processing unit (1416) for decrypting and extracting said license key with said second private decryption key based on a result of the decryption by said second decryption processing unit, and

a first authentication data holding unit (1442) for encrypting first authentication data containing at least said first public encryption key in a manner decodable with a public authentication key, and holding the encrypted first authentication data for external output; and

said content data supply device further includes:

a first authentication decryption processing unit (326) for decrypting and extracting said externally applied first authentication data decodable with said public authentication key, and

a distribution control unit (312) for performing authentication processing based on said first authentication data extracted by said first authentication decryption processing unit, and determining at least whether the license key is to be distributed or not.

18. The data distribution system according to claim 17, wherein

said memory unit includes first memory means (1412) for storing said license key and said encrypted content data each decrypted by said second decryption processing unit into a form decodable with said second private decryption key.

19. The data distribution system according to claim 17, wherein said memory unit includes:

first memory means (1412) for storing said encrypted content data, and

second memory means (1500) for storing said license key decrypted by said third decryption processing unit.

20. The data distribution system according to claim 17, wherein said distributed data decoding unit is a memory card releasably attached to said terminal,

said first private decryption key takes a value predetermined depending on the type of said memory card, and

said second private decryption key is unique to each of said memory cards.

21. The data distribution system according to claim 17, wherein said first private decryption key takes a value predetermined depending on a type of said distributed data decoding unit, and

said second private decryption key is unique to said distributed data decoding unit.

22. The data distribution system according to claim 17, wherein each of said terminals further includes a content reproducing unit, and

said content reproducing unit further includes a second authentication data holding unit (1525) for encrypting second authentication data including at least a predetermined third public encryption key into a form decodable with said public authentication key, and holding the encrypted second authentication data for external output.

23. The data distribution system according to claim 22, wherein said first authentication decryption processing unit further decrypts said second authentication data encrypted into a form decodable with said

public authentication key, and outputs the said second authentication data, and

said distribution control unit performs authentication based on said first and second authentication data extracted by said first authentication decryption processing unit, and determines at least whether the license key is to be distributed or not.

24. The data distribution system according to claim 17, wherein said first and second interface units are connected over a cellular phone network.

25. The data distribution system according to claim 17, wherein said first interface unit includes a connecting unit directly connectable to said terminal.

26. The data distribution system according to claim 20, wherein said first interface unit includes a connecting unit directly connectable to said data storing unit.

27. The data distribution system according to claim 26, wherein said distributed data decoding unit includes a plurality of terminals (1462.0 - 1462.3) for receiving data from said connecting unit, and

the number of the terminals receiving the data from said connecting unit is changeable in accordance with an externally applied instruction.

28. The data distribution system according to claim 22, wherein said memory unit receives the output of said second decryption processing unit, and stores said license key encrypted into a form decodable with said second private decryption key;

said content reproducing unit includes:

a fourth key holding unit (1520) for holding a third private decryption key used for decrypting the data encrypted with said third public encryption key,

a fourth decryption processing unit (1522) for decrypting and extracting said second symmetric key externally encrypted with said third public encryption key,

a third session key generating unit (1502) for producing a third symmetric key,

a second encryption processing unit (1504) for encrypting said third symmetric key based on said second symmetric key decrypted and extracted by said fourth decryption processing unit,

a fifth decryption processing unit (1506) for decrypting and extracting the license key encrypted outside said content reproducing unit based on said third symmetric key, and

a data reproducing unit (1508) for decrypting and reproducing the encrypted content data recorded in said memory unit with said extracted license key;

said distributed data decoding unit includes:

a second authentication decryption processing unit (1452) for extracting said third public encryption key by decrypting said second authentication data taking an encrypted form decodable with said public authentication key and applied from said content reproducing unit,

a third encryption processing unit (1430) for encrypting said second symmetric key produced by said second session key generating unit based on said third public encryption key, and

a control unit (1420) for instructing said first encryption processing unit to receive said third symmetric key encrypted with said second symmetric key by said content reproducing unit, encrypt said license key prepared by decrypting the data stored in said memory unit with said second private decryption key, based on said third symmetric key decrypted by said second decryption processing unit (1410) based on said second symmetric key, and output the encrypted license key to said content reproducing unit; and

said control unit performs the authentication based on said second authentication data decrypted by said second authentication decryption processing unit, and determines whether at least the license key is to be

~~output or not.~~

29. The data distribution system according to claim 20, wherein said memory unit receives the output of said second decryption processing unit, and stores said license key encrypted into a form decodable with said second private decryption key;

said distributed data decoding unit includes:

a second authentication decryption processing unit (1452) operating, for transferring at least said license key to a different distributed data decoding unit of another terminal, in accordance with the transfer processing instructed externally with respect to said distributed data decoding unit to decrypt with said public authentication key the first authentication data in an encrypted form decodable with said public authentication key applied from said different distributed data decoding unit, and extract said first public encryption key in said different distributed data decoding unit,

a third encryption processing unit (1430) for encrypting said second symmetric key with said first public encryption key of said different distributed data decoding unit, and

a fourth encryption processing unit (1414) for performing encryption wit the second public encryption key of said different distributed data decoding unit;

said second session key generating unit generates said second symmetric key in accordance with said transfer processing;

said second decryption processing unit operates in accordance with said transfer operation to decrypt and extract a fourth symmetric key encrypted with said second symmetric key and applied from said different distributed data decoding unit and the second public encryption key of said different distributed data decoding unit;

said third decryption processing unit operates in accordance with said transfer processing to decrypt, based on said second private decryption key, the data encrypted with said second public encryption key stored in said memory unit, and extract the license key;

said fourth encryption processing unit operates in accordance with said transfer processing to encrypt said extracted license key based on said second private decryption key of said different distributed data decoding unit;

said first decryption processing unit operates in accordance with said transfer processing to encrypt the output of said fourth encryption processing unit with said fourth symmetric key, and output the encrypted output to said different distributed data decoding unit; and

said control means performs authentication processing based on the second authentication data output from said different data decoding unit and extracted by said authentication decryption processing unit, and determines at least whether the license key is to be output or not.

30. The data distribution system according to claim 29, wherein

said different distributed data decoding unit operates in said authentication decrypting processing such that said first authentication data holding unit outputs said first authentication data in accordance with the transfer operation instructed outside externally with respect to said different distributed data decoding unit for transferring at least said license key from said distributed data decoding unit;

said first decryption processing unit operates in accordance with said transfer processing to decrypt and extract said second symmetric key encrypted with said first public encryption key applied from said distributed data decoding unit and generated by said distributed data decoding unit;

said second session key generating unit generates said fourth symmetric key in accordance with said transfer acceptance processing;

said first encryption processing unit operates in accordance with said transfer acceptance processing to encrypt and output said second public encryption key and said fourth symmetric key based on said second symmetric key; and

said second public decryption processing unit decrypts the license key encrypted with said second public encryption key in said distributed

data decoding unit and further encrypted with said fourth symmetric key, and recording the decoded license key in said memory unit.

31. The data distribution system according to claim 26, wherein said content data supply device further includes:

a fifth key holding unit for holding a fifth symmetric key common to said content reproducing unit, and

a third license encryption processing unit for encrypting said license key based on said fifth symmetric key held by said fifth key holding unit, and outputting said encrypted license key to said first license encryption processing unit; and

said content reproducing unit further includes:

sixth key holding means for holding said fifth symmetric key, and

a fifth decryption processing unit arranged between said fourth decryption processing unit and said data reproducing unit for decrypting the output of said fourth decryption processing unit with said fifth symmetric key held by said sixth key holding unit to extract and output said license key to said data reproducing unit.

32. The data distribution system according to claim 26, wherein said content data supply device further includes:

a fifth key holding unit for holding a fourth public encryption key allowing decoding by said content reproducing unit, and

a third license encryption processing unit for encrypting said license key based on said fourth public encryption key to output the encrypted license key to said first license key encryption processing unit; and

said content reproducing unit further includes:

sixth key holding means for holding a fourth private decryption key allowing decryption of the data encrypted with the fourth public encryption key, and

a fifth decryption processing unit arranged between said fourth decryption processing unit and said data reproducing unit for decrypting the output of said fourth decryption processing unit with the fourth private

decryption key to extract and output said license key to said data reproducing unit.

33. The data distribution system according to claim 20, wherein said terminal includes a plurality of distributed data decoding unit.

EP ・ US

特 許 協 力 条 約

PCT

国際調査報告

(法８条、法施行規則第40、41条)
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人の書類記号　９００３９１	今後の手続きについては、国際調査報告の送付通知様式(ＰＣＴ／ＩＳＡ／２２０)及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０５７７０	国際出願日 (日.月.年)　２５．０８．００	優先日 (日.月.年)　２７．０８．９９
出願人（氏名又は名称） 富士通株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　3　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎
ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ⅰ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　5　図とする。☒ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査[redacted]　　国際出願番[redacted]PCT／JP00／05770

A.　発明の属する分野の分類（国際特許分類（IPC））
Int Cl' G10K15／02, G06F15／00, G06F17／60, H04L9／08, H04L9／10, G06K19／00, H04H1／00, H04M3／42, H04M3／493, H04M11／08, G10L19／00, G06F13／00, H04L12／22, H04L12／58

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int Cl' G10K15／00～15／06, G10L19／00～19／14, H04L9／00～9／38, G09C1／00～5／00, G06F12／00, G06F12／14, G06K19／00, H04M11／00～11／08

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1926～1995年
日本国公開実用新案公報　1971～2000年
日本国登録実用新案公報　1994～2000年
日本国実用新案登録公報　1996～2000年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
INSPEC（DIALOG）
WPI（DIALOG）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	EP, 561685, A2(FUJITSU LIMITED), 22.9月.1993(22.09.93), 全文全図, &US,5392351,A &US,5555304,A &US, 5796824,A &JP,5-257816,A &JP,3073590,B2	1-33
A	JP, 62－53042, A(日本電信電話株式会社), 7.3月.1987(07.03.87), 全文全図(ファミリーなし)	1-33
A	JP, 8－186667, A(松下電器産業株式会社), 16.7月.1996(16.07.96), 全文全図(ファミリーなし)	1-33

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
10.11.00	21.11.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	松尾　淳一　印　5C　8842 電話番号　03－3581－1101　内線　3540

様式PCT／ISA／210（第2ページ）（1998年7月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	ＪＰ，８－６９４１９，Ａ(株式会社島津製作所)，12.3月.1996(12.03.96)，全文全図(ファミリーなし)	1-33
E，A	ＪＰ，１１－３２８０３３，Ａ(富士通株式会社)，30.11月.1999(30.11.99)，全文全図(ファミリーなし)	1-33
A	日経エレクトロニクス，No.739，「小型メモリ・カードで音楽著作権を守る」，22.3月.1999(22.03.99)，p.49-53	1-33
A	日経エレクトロニクス，No.728，「米周辺機器メーカ大手が，ＭＰ３携帯型プレーヤ発売　著作権対策は付加せず」，19.10月.1998(19.10.98)，p.31-32	1-33
A	日経エレクトロニクス，No.731，「汚れたイメージ払拭ねらうＭＰ３業界 音楽配信の会議 Webnoise から」，30.11月.1998(30.11.98)，p.29-30	1-33

56/prts

DESCRIPTION

Data Distribution System

Technical Field

The present invention relates to a data distribution system for distributing information to terminals such as cellular phones, and particularly to a data distribution system, which can secure a copyright relating to copied information.

Background Art

By virtue of the progress in information communication networks and the like such as the Internet in these few years, each user can now easily access network information through individual-oriented terminals employing a cellular phone or the like.

In such information communication, information is transmitted through digital signals. It is now possible to obtain copied music and video information transmitted via the aforementioned information communication network without degradation in the audio quality and picture quality of the copy data, even in the case where an individual user performs the copy.

Thus, there is a possibility of the copyright of the copyright owner being significantly infringed unless some appropriate measures to protect copyrights are taken when any content data subject to copyright protection such as music data and image data is to be transmitted on the information communication network.

However, if copyright protection is given top priority so that distribution of content data through the disseminating digital information communication network is suppressed, the copyright owner who can essentially collect a predetermined copyright royalty for copies of a copyrighted work will also incur some disbenefit.

Instead of the distribution over the digital information communication network described above, distribution may be performed via

record mediums storing digital data. In connection with the latter case, music data stored in CDs (compact disks) on the market can be freely copied in principle into magneto-optical disks (e.g., MDs) as long as the duplication is only for the personal use. However, a personal user performing digital recording or the like indirectly pays predetermined amounts in prices of the digital recording device itself and the medium as guaranty moneys to a copyright holder.

However, the music data is digital data, which does not cause deterioration of information when it is copied as digital signals from a CD to an MD. Therefore, for the copyright protection, such structures are employed that the music information cannot be copied as digital data from the recordable MD to another music data.

Under present circumstances, therefore, digital data can be freely copied from a CD to an MD, i.e., from a master of digital record medium to a slave, but cannot be copied from a recordable MD to another MD.

In view of the above, the public distribution itself of the music data and image data over the digital information communication network is restricted by the public transmission right of the copyright holder, and therefore sufficient measures must be taken for the copyright protection.

For the above case, it is naturally necessary to inhibit such an act that a user, who is not originally authorized, receives copyrighted data distributed to the public over the information communication network. Further, it is necessary to inhibit such an act that copyrighted data, which was once received by an authorized user, is further duplicated without authorization.

Disclosure of the Invention

An object of the invention is to provide an information distribution system for distributing copyrighted data over an information network such a cellular phone network, and particularly an information distribution system, in which only users having proper access rights can receive such information.

Another object of the invention is to provide an information

distribution system, which can protect distributed copyrighted data from being duplicated without authorization from a copyright holder.

For achieving the above objects, the invention provides a data distribution system for distributing encrypted content data to each of terminals of a plurality of users from a content data supply device.

The content data supply device includes a first interface unit, a first session key generating unit, a session key encryption processing unit, a session key decrypting unit, a first license data encryption processing unit and a second license data encryption processing unit.

The first interface unit externally transmits data.

The first session key generating unit produces a first symmetric key to be updated in response to every transmission of the encrypted content data. The session key encryption processing unit encrypts the first symmetric key with a first public encryption key predetermined corresponding to the user's terminal, and applies the same to the first interface unit. The session key decrypting unit decrypts returned data encrypted with the first symmetric key.

The first license data encryption processing unit encrypts a license key for decrypting the encrypted content data using, as key data, the data decrypted by the session key decrypting unit. The second license data encryption processing unit further encrypts an output of the first license data encryption processing unit with a second symmetric key, and applies the same to the first interface unit for distribution.

Each of the terminals includes a second interface unit and a distributed data decoding unit.

The second interface unit externally transmits the data.

The distributed data decoding unit receives and stores the encrypted content data. The distributed data decoding unit includes a first key holding unit, a first decryption processing unit, a second key holding unit, a first encryption processing unit, a second decryption processing unit, a first memory unit, a third key holding unit and a third decryption processing unit.

The first key holding unit holds a first private decryption key for

decrypting the data encrypted by the first public encryption key, and the first decryption processing unit receives and decrypts the first symmetric key encrypted with the first public encryption key.

The second key holding unit holds a second public encryption key. The first encryption processing unit encrypts the second public encryption key based on the first symmetric key, and outputs the same to the second interface unit.

The second decryption processing unit receives the license key encrypted by the second license data encryption processing unit, and decrypts the same based on the second symmetric key.

The first memory unit stores the encrypted content data allowing decryption based on the license key.

The third key holding unit holds a second private decryption key for decrypting the data encrypted with the second public encryption key. The third decryption processing unit decrypts the license key with the second private decryption key based on a result of the decryption by the second decryption processing unit.

According to another aspect, the invention provides a data distribution system for distributing at least one of encrypted data and a license key for decrypting the decrypted data from a content data supply device to each of terminals of a plurality of users.

The content data supply device includes a first interface unit, a first session key generating unit, a session key encryption processing unit, a session key decrypting unit, a first license data encryption processing unit and a second license data encryption processing unit.

The first interface unit externally transmits data.

The first session key generating unit produces a first symmetric key to be updated in response to every transmission of the encrypted content data. The session key encryption processing unit encrypts the first symmetric key with a first public encryption key predetermined corresponding to the user's terminal, and applies the same to the first interface unit. The session key decrypting unit decrypts and extracts a second symmetric key and a second public encryption key both encrypted

with the first symmetric key and returned.

The first license data encryption processing unit encrypts a license key for decrypting the encrypted content data with the second public encryption key decrypted by the session key decrypting unit. The second license data encryption processing unit further encrypts an output of the first license data encryption processing unit with the second symmetric key, and applies the same to the first interface unit for distribution.

Each of the terminals includes a second interface unit and a distributed data decoding unit.

The second interface unit externally transmits the data.

The distributed data decoding unit receives and stores the encrypted content data and the license key.

The distributed data decoding unit includes a first key holding unit, a first decryption processing unit, a second key holding unit, a second session key generating unit, a first encryption processing unit, a second decryption processing unit, a memory unit, a third key holding unit, a third decryption processing unit and a first authentication data holding unit.

The first key holding unit holds a first private decryption key for decrypting the data encrypted by the first public encryption key, and the first decryption processing unit receives and decrypts the first symmetric key encrypted with the first public encryption key.

The second key holding unit holds a second public encryption key. The second session key generating unit produces a second symmetric key.

The first encryption processing unit encrypts the second public encryption key and the second symmetric key based on the first symmetric key, and outputs the same to the second interface unit. The second encryption processing unit receives the license key encrypted by the license data encryption processing unit, and decrypts the same based on the second symmetric key. The memory unit stores the encrypted content data decodable with the license key.

The third key holding unit holds a second private decryption key for decrypting the data encrypted with the second public encryption key. The third decryption processing unit decrypts the license key with the second

private decryption key based on a result of the decryption by the second decryption processing unit, and extracts the same. The first authentication data holding unit can encrypt first authentication data containing at least the first public encryption key in a manner decodable with a public authentication key, and holds the same for external output.

The content data supply device further includes a first authentication decryption processing unit for decrypting and extracting the externally applied first authentication data decodable with the public authentication key, and a distribution control unit for performing authentication processing based on the first authentication data extracted by the first authentication decryption processing unit, and determining at least whether the license key is to be distributed for not.

According to the invention, therefore, only a regular or proper user can receive the content data for storing it in the memory. Further, the system is configured as follows. When data once stored in a memory card of an owner is copied for use by another person, the data of the owner or sender changes into an irreproducible form. Therefore, the system can prevent the copyright holder from sustaining drawbacks due to unlimited copying.

According to another advantage of the invention, the license key is distributed to only the authorized terminal so that the copyright protection is further enhanced.

According to further another advantage of the invention, the user can purchase encrypted content data from a content data vending machine without utilizing a distribution carrier. This further improves convenience to users.

The foregoing and other objects, features, aspects and advantages of the present invention will become more apparent from the following detailed description of the present invention when taken in conjunction with the accompanying drawings.

Brief Description of the Drawings

Fig. 1 conceptually and schematically shows a whole structure of an

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年3月8日 (08.03.2001)

PCT

(10) 国際公開番号
WO 01/16932 A1

(51) 国際特許分類[7]: G10K 15/02, G06F 15/00, 17/60, H04L 9/08, 9/10, G06K 19/00, H04H 1/00, H04M 3/42, 3/493, 11/08, G10L 19/00, G06F 13/00, H04L 12/22, 12/58

(21) 国際出願番号: PCT/JP00/05770

(22) 国際出願日: 2000年8月25日 (25.08.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/241747 1999年8月27日 (27.08.1999) JP
特願平11/345229 1999年12月3日 (03.12.1999) JP

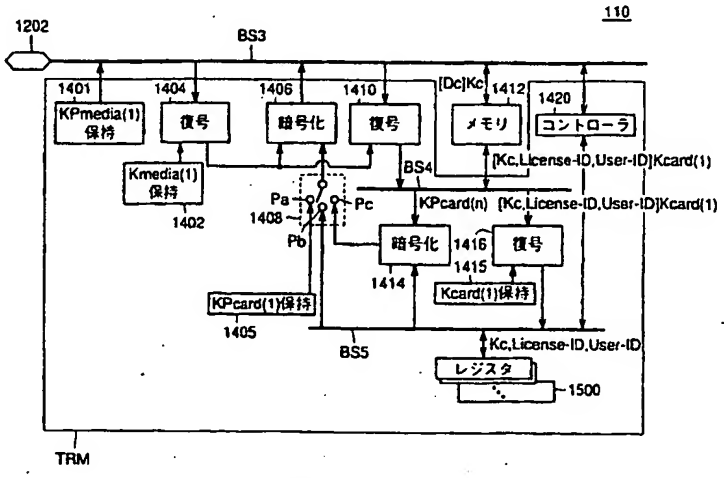
(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP). 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 Tokyo (JP). 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 畑中正行 (HATANAKA, Masayuki) [JP/JP]. 蒲田 順 (KAMADA, Jun) [JP/JP]. 畠山卓久 (HATAKEYAMA, Takahisa) [JP/JP]. 長谷部高行 (HASEBE, Takayuki) [JP/JP]. 小谷誠剛 (KOTANI, Seigou) [JP/JP]. 古田茂樹 (FURUTA, Shigeki) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 木下泰三 (KINOSHITA, Taizou) [JP/JP]; 〒187-8588 東京都小平市上水本町五丁目20番1号 株式会社 日立製作所 半導体グ

[続葉有]

(54) Title: DATA DISTRIBUTION SYSTEM

(54) 発明の名称: データ配信システム



1402...HOLD Kmedia(1)
1404...DECRYPT
1405...HOLD Kpcard(1)
1406...ENCRYPT
1410...HOLD Kpmedia(1)
1410...DECRYPT
1412...MEMORY
1414...ENCRYPT
1415...HOLD Kpcard(1)
1416...DECRYPT
1420...CONTROLLER
1500...REGISTER

(57) Abstract: A memory card (110) extracts a session key (Ks) by decoding data provided on a data bus (BS3) through a cellular network from a server. Encryption means (1406) encrypts a public key KPcard (1) of the memory card (110) based on the session key Ks and sends it to the server over the data bus (BS3). A register (1500) stores decrypted data, such as a license ID and a user ID, and a memory (1412) stores content data ([Dc]Kc) encrypted by the license key (Kc) and supplied over the data bus (BS3).

[続葉有]

WO 01/16932 A1

ループ内 Tokyo (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内 Tokyo (JP). 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI, Miwa) [JP/JP]. 堀　吉宏 (HORI, Yoshihiro) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP).

(74) 代理人: 深見久郎, 外(FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

メモリカード１１０は、サーバから携帯電話網を介してデータバスＢＳ３に与えられるデータから、復号処理をすることによりセッションキーＫｓを抽出する。暗号化処理部１４０６は、セッションキーＫｓに基づいて、メモリカード１１０の公開暗号化鍵ＫＰｃａｒｄ（１）を暗号化してデータバスＢＳ３を介してサーバに与える。レジスタ１５００は、復号されたライセンスＩＤ、ユーザＩＤ等のデータをサーバから受けとって格納し、メモリ１４１２は、データバスＢＳ３からライセンスキーＫｃにより暗号化されている暗号化コンテンツデータ［Ｄｃ］Ｋｃを受けて格納する。

明細書

データ配信システム

技術分野

本発明は、携帯電話等の端末に対して情報を配送するためのデータ配信システムに関し、より特定的には、コピーされた情報に対する著作権保護を可能とするデータ配信システムに関するものである。

背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタル情報を記録した記録媒体を例にとって考えてみると、通常販売されている音楽情報を記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行な

う個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

しかも、ＣＤからＭＤへデジタル信号である音楽情報をコピーした場合、これらの情報がコピー劣化のほとんどないデジタル情報であることに鑑み、１つのＭＤからさらに他のＭＤに音楽データをデジタル情報としてコピーすることは、著作権者保護のために機器の構成上できないようになっている。

すなわち、現状においては、デジタル記録媒体であるＣＤからＭＤへのコピーは、親から子へのコピーは自由に行なうことができるものの、記録可能なＭＤからＭＤへのコピーを行なうことはできない。

そのような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

この場合、情報通信網を通じて公衆に送信される著作物データを、本来受信する権限のないユーザが受信することを防止する必要があるのはもちろんのこと、仮に権限を有するユーザが受信を行なった場合でも、一度受信された著作物が、さらに勝手に複製されることを防止することも必要となる。

発明の開示

本発明の目的は、情報通信網、たとえば携帯電話等の情報通信網を介して著作物データを配信する場合に、正当なアクセス権を有するユーザのみがこのような情報を受信することが可能な情報配信システムを提供することである。

この発明の他の目的は、配信された著作物データが、著作権者の許可なく複製されることを防止することが可能な情報配信システムを提供することである。

係る目的を達成するために本願発明に係るデータ配信システムは、コンテンツデータ供給装置から、暗号化コンテンツデータを複数のユーザの各端末に配信するためのデータ配信システムである。

コンテンツデータ供給装置は、第１のインタフェース部と、第１のセッションキー発生部と、セッションキー暗号化部と、セッションキー復号部と、第１のライセンスデータ暗号化処理部と、第２のライセンスデータ暗号化処理部とを備え

る。

第１のインタフェース部は、外部との間でデータを授受する。

第１のセッションキー発生部は、暗号化コンテンツデータの通信ごとに更新される第１の共通鍵を生成する。セッションキー暗号化部は、ユーザの端末に対応して予め定められた第１の公開暗号化鍵により第１の共通鍵を暗号化して第１のインタフェース部に与える。セッションキー復号部は、第１の共通鍵により暗号化されて返信されるデータを復号する。

第１のライセンスデータ暗号化処理部は、暗号化コンテンツデータを復号するためのライセンスキーを、セッションキー復号部により復号されたデータを鍵データとして暗号化する。第２のライセンスデータ暗号化処理部は、第１のライセンスデータ暗号化処理部の出力を第２の共通鍵でさらに暗号化して第１のインタフェース部に与え配信する。

各端末は、第２のインタフェース部と、配信データ解読部とを備える。

第２のインタフェース部は、外部との間でデータを授受する。

配信データ解読部は、暗号化コンテンツデータを受けて格納する。配信データ解読部は、第１の鍵保持部と、第１の復号処理部と、第２の鍵保持部と、第１の暗号化処理部と、第２の復号処理部と、第１の記憶部と、第３の鍵保持部と、第３の復号処理部とを備える。

第１の鍵保持部は、第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の復号処理部は、第１の公開暗号化鍵によって暗号化された第１の共通鍵を受けて、復号処理する。

第２の鍵保持部は、第２の公開暗号化鍵を保持する。第１の暗号化処理部は、第２の公開暗号化鍵を、第１の共通鍵に基づいて暗号化し、第２のインタフェース部に出力する。

第２の復号処理部は、第２のライセンスデータ暗号化処理部からの暗号化されたライセンスキーを受け、第２の共通鍵に基づいて復号化する。

第１の記憶部は、ライセンスキーに基づいて復号できる前記暗号化コンテンツデータを格納する。

第３の鍵保持部は、第２の公開暗号化鍵によって暗号化されたデータを復号化

するための第２の秘密復号鍵を保持する。第３の復号処理部は、第２の復号処理部での復号結果に基づいて、第２の秘密復号鍵によりライセンスキーを復号するためのを備える。

この発明のさらに他の局面に従うと、コンテンツデータ供給装置から、暗号化コンテンツデータと暗号化データを復号するためのライセンスキーとのうちの少なくとも１つを複数のユーザの各端末に配信するためのデータ配信システムである。

コンテンツデータ供給装置は、第１のインタフェース部と、第１のセッションキー発生部と、セッションキー暗号化処理部と、セッションキー復号部と、第１のライセンスデータ暗号化処理部と、第２のライセンス暗号化処理部とを備える。

第１のインタフェース部は、外部との間でデータを授受する。

第１のセッションキー発生部は、暗号化コンテンツデータの通信ごとに更新される第１の共通鍵を生成する。セッションキー暗号化処理部は、ユーザの端末に対応して予め定められた第１の公開暗号化鍵により第１の共通鍵を暗号化して第１のインタフェース部に与える。セッションキー復号部は、第１の共通鍵により暗号化されて返信される第２の共通鍵と第２の公開暗号化鍵を復号し抽出する。

第１のライセンスデータ暗号化処理部は、暗号化コンテンツデータを復号するためのライセンスキーを、セッションキー復号部により復号された第２の公開暗号化鍵により暗号化する。第２のライセンス暗号化処理部は、第１のライセンスデータ暗号化処理部の出力を第２の共通鍵でさらに暗号化して第１のインタフェース部に与え配信する。

各端末は、第２のインタフェース部と、配信データ解読部とを備える。

第２のインタフェース部は、外部との間でデータを授受する。

配信データ解読部は、暗号化コンテンツデータおよびライセンスキーを受けて格納する。

配信データ解読部は、第１の鍵保持部と、第１の復号処理部と、第２の鍵保持部と、第２のセッションキー発生部と、第１の暗号化処理部と、第２の復号処理部と、記憶部と、第３の鍵保持部と、第３の復号処理部と、第１の認証データ保

持部とを備える。

第１の鍵保持部は、第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する。第１の復号処理部は、第１の公開暗号化鍵によって暗号化された第１の共通鍵を受けて、復号処理する。

第２の鍵保持部は、第２の公開暗号化鍵を保持する。第２のセッションキー発生部は、第２の共通鍵を生成する。

第１の暗号化処理部は、第２の公開暗号化鍵と第２の共通鍵を、第１の共通鍵に基づいて暗号化し、第２のインタフェース部に出力する。第２の復号処理部は、第２のライセンスデータ暗号化処理部からの暗号化されたライセンスキーを受け、第２の共通鍵に基づいて復号する。記憶部は、ライセンスキーにて復号可能な暗号化コンテンツデータを格納する。

第３の鍵保持部は、第２の公開暗号化鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する。第３の復号処理部は、第２の復号処理部での復号結果に基づいて、第２の秘密復号鍵によりライセンスキーを復号し抽出する。第１の認証データ保持部は、第１の公開暗号化鍵を少なくとも含む第１の認証データを公開認証鍵により復号できるように暗号化して保持し外部に出力可能である。

コンテンツデータ供給装置は、公開認証鍵により復号でき、かつ外部から与えられる第１の認証データを復号して抽出するための第１の認証復号処理部と、第１の認証復号処理部により抽出された第１の認証データに基づいて認証処理を行ない、少なくともライセンスキーを配信するか否かを判断する配信制御部をさらに含む。

したがって、本発明によれば、正規のユーザのみがコンテンツデータを受信してメモリ中に格納することが可能となる。しかも、１度メモリカード中に格納されたデータを、他人にコピーさせる場合は、当該他人が再生可能な状態でデータを移植するためには、送信元においては、データの再生が不能となってしまう構成となっているので、無制限なコピーにより著作権が不当な不利益を被るのを防止することが可能となる。

この発明の他の利点は、認証された端末にのみライセンスキーが配信されるの

で、著作権の保護が一層強化されることである。

この発明のさらに他の利点は、ユーザが配信キャリアを介してではなく、コンテンツデータ販売機により暗号化コンテンツデータを購入することができるので、ユーザの利便性が一層向上することである。

図面の簡単な説明

図１は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

図２は、図１に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明する図である。

図３は、図１に示した配信サーバ１０の構成を示す概略ブロック図である。

図４は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

図５は、図４に示したメモリカード１１０の構成を説明するための概略ブロック図である。

図６は、図１および図３～図５で説明したデータ配信システムにおける配信モードを説明するための第１のフローチャートである。

図７は、図１および図３～図５で説明したデータ配信システムにおける配信モードを説明するための第２のフローチャートである。

図８は、携帯電話機１００内においてコンテンツデータを再生し、、音楽として外部に出力するための再生処理を説明するフローチャートである。

図９は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１のフローチャートである。

図１０は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第２のフローチャートである。

図１１は、実施の形態２のメモリカード１２０に対応した音楽サーバ３１の構成を示す概略ブロック図である。

図１２は、実施の形態２における携帯電話機１０１の構成を説明するための概略ブロック図である。

図１３は、本発明の実施の形態２のメモリカード１２０の構成を説明するための概略ブロック図である。

図１４は、図１３で説明したメモリカード１２０を用いた配信モードを説明するための第１のフローチャートである。

図１５は、図１３で説明したメモリカード１２０を用いた配信モードを説明するための第２のフローチャートである。

図１６は、携帯電話機１０１内においてコンテンツデータを再生し、音楽として外部に出力するための再生処理を説明する第１のフローチャートである。

図１７は、携帯電話機１０１内においてコンテンツデータを再生し、音楽として外部に出力するための再生処理を説明する第２のフローチャートである。

図１８は、２つのメモリカード間でコンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１のフローチャートである。

図１９は、２つのメモリカード間でコンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第２のフローチャートである。

図２０は、実施の形態３のデータ配信システムの構成を説明するための概念図である。

図２１は、実施の形態３のコンテンツデータ販売機２０００の構成を示す概略ブロック図である。

図２２は、図２０および図２１で説明したデータ配信システムにおける配信モードを説明するための第１のフローチャートである。

図２３は、図２０および図２１で説明したデータ配信システムにおける配信モードを説明するための第２のフローチャートである。

図２４は、実施の形態３の変形例のコンテンツデータ販売機２００１の構成を示す概念図である。

図２５は、実施の形態３の変形例のデータ配信システムにおける配信モードを説明するための第１のフローチャートである。

図２６は、実施の形態３の変形例のデータ配信システムにおける配信モードを

説明するための第２のフローチャートである。

図２７は、実施の形態４のコンテンツデータ販売機３０００の構成を説明するための概略ブロック図である。

図２８は、図２７で説明したデータ配信システムにおける配信モードを説明するための第１のフローチャートである。

図２９は、図２７で説明したデータ配信システムにおける配信モードを説明するための第２のフローチャートである。

図３０は、実施の形態４の変形例のデータ配信システムにおける配信モードを説明するための第１のフローチャートである。

図３１は、実施の形態４の変形例のデータ配信システムにおける配信モードを説明するための第２のフローチャートである。

図３２は、実施の形態５における携帯電話機１０５の構成を説明するための概略ブロック図である。

図３３は、実施の形態５のメモリカード１４０に対応した配信サーバ１２の構成を示す概略ブロック図である。

図３４は、本発明の実施の形態５のメモリカード１４０の構成を説明するための概略ブロック図である。

図３５は、メモリカード１４０を用いた配信モードを説明するための第１のフローチャートである。

図３６は、メモリカード１４０を用いた配信モードを説明するための第２のフローチャートである。

図３７は、メモリカード１４０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第１のフローチャートである。

図３８は、メモリカード１４０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第２のフローチャートである。

図３９は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１のフローチャートであ

る。

図４０は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第２のフローチャートである。

図４１は、本発明の実施の形態６のコンテンツデータ販売機３０１０の構成を示す概略ブロック図である。

図４２は、コンテンツデータ販売機３０１０を用いたデータ配信システムにおける配信モードを説明するための第１のフローチャートである。

図４３は、コンテンツデータ販売機３０１０を用いたデータ配信システムにおける配信モードを説明するための第２のフローチャートである。

図４４は、実施の形態７における携帯電話機１０７の構成を説明するための概略ブロック図である。

図４５は、実施の形態７の携帯電話機１０７に対応した配信サーバ１３の構成を示す概略ブロック図である。

図４６は、配信サーバ１２と携帯電話機１０７を用いた配信モードを説明するための第１のフローチャートである。

図４７は、配信サーバ１２と携帯電話機１０７を用いた配信モードを説明するための第２のフローチャートである。

図４８は、メモリカード１４０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第１のフローチャートである。

図４９は、メモリカード１４０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第２のフローチャートである。

図５０は、実施の形態７において、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１のフローチャートである。

図５１は、実施の形態７において、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第

２のフローチャートである。

図５２は、本発明の実施の形態８のコンテンツデータ販売機３０２０の構成を示す概略ブロック図である。

図５３は、コンテンツデータ販売機３０２０を用いたデータ配信システムにおける配信モードを説明するための第１のフローチャートである。

図５４は、コンテンツデータ販売機３０２０を用いたデータ配信システムにおける配信モードを説明するための第２のフローチャートである。

図５５は、メモリカード１４０の端子１２０２部分の構成を説明する概略ブロック図である。

図５６は、メモリカード１４０の端子１２０２部分の構成の変形例を説明するための概略ブロック図である。

発明を実施するための最良の形態

以下、本発明の実施例を図面とともに説明する。

［実施例１］

［システムの全体構成］

図１は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

なお、以下では携帯電話網を介して、音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物データ、たとえば画像データ等の著作物データを、他の情報通信網を介して配信する場合にも適用することが可能なものである。

図１を参照して、著作権の存在する音楽情報を管理する配信サーバ１０は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリア２０である携帯電話会社に、このような暗号化データを与える。一方、認証サーバ１２は、音楽データの配信を求めてアクセスしてきた機器が正規の機器であるか否かの認証を行なう。

配信キャリア２０は、自己の携帯電話網を通じて、各ユーザからの配信要求

(配信リクエスト) を配信サーバ１０に中継する。配信サーバ１０は、配線リクエストがあると、認証サーバ１２により正規の機器からのアクセスであることを確認し、要求されたコンテンツデータをさらに暗号化したうえで、配信キャリア２０の携帯電話網を介して、各ユーザの携帯電話機に対して配信する。

図１においては、たとえば携帯電話ユーザ１の携帯電話機１００には、携帯電話機１００により受信された暗号化コンテンツデータを受取って、上記送信にあたって行なわれた暗号化については復号化したうえで、携帯電話機１００中の音楽再生部（図示せず）に与えるための着脱可能なメモリカード１１０に格納する構成となっている。

さらに、たとえばユーザ１は、携帯電話機１００に接続したヘッドホン１３０等を介してこのようなコンテンツデータを再生した音楽を聴取することが可能である。

以下では、このような配信サーバ１０と認証サーバ１２と配信キャリア２０とを併せて、音楽サーバ３０と総称することにする。

また、このような音楽サーバ３０から、各携帯電話端末等にコンテンツデータを伝送する処理を「配信」と称することとする。

このような構成とすることで、まず、正規のメモリカードであるメモリカード１１０を購入していない正規のユーザでないものは、音楽サーバ３０からの配信データを受取って再生することが困難な構成となる。

しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

しかも、このようなコンテンツデータの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

このとき、たとえばメモリカード１１２を有するユーザ２が、自己の携帯電話機１０２により、音楽サーバ３０から直接コンテンツデータの配信を受けること

は可能である。しかしながら、相当量の情報量を有するコンテンツデータ等をユーザ２が直接音楽サーバ３０から受信することとすると、その受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けているユーザ１から、そのコンテンツデータをコピーできることを可能としておけば、ユーザにとっての利便性が向上する。

しかしながら、著作権者の権利保護の観点からは、自由なコンテンツデータのコピーを放任することはシステム構成上許されない。

図１に示した例では、ユーザ１が受信したコンテンツデータを、コンテンツデータそのものおよび当該コンテンツデータを再生可能とするために必要な情報とともに、ユーザ２に対してコピーさせる場合をコンテンツデータの「移動」と呼ぶ。この場合、ユーザ１は、再生のために必要な情報（再生情報）ごとユーザ２にコピーさせるため、情報の移動を行なった後には、ユーザ１においてはコンテンツデータの再生を行なうことは不可能とする必要がある。ここで、コンテンツデータは所定の暗号化方式にしたがって暗号化された暗号化コンテンツデータとして配信され、「再生情報」とは、後に説明するように、上記所定の暗号化方式にしたがって暗号化コンテンツデータを復号可能な鍵（ライセンスキーとも称する）と、著作権保護に関わる情報であるライセンスＩＤデータやユーザＩＤデータ等のライセンス情報とを意味する。

これに対して、コンテンツデータのみを暗号化されたままの状態で、ユーザ２にコピーさせることを音楽情報の「複製」と呼ぶこととする。

この場合、ユーザ２の端末には、このようなコンテンツデータを再生させるために必要な再生情報はコピーされないので、ユーザ２は、暗号化コンテンツデータを得ただけでは、音楽を再生させることができない。したがって、ユーザ２が、このような音楽の再生を望む場合は、改めて音楽サーバ３０からコンテンツデータの再生を可能とするための再生情報の配信を受ける必要がある。しかしながら、この場合は、再生を可能とするための情報の配信のみを受ければよいため、ユーザ２が直接音楽サーバ３０からすべての配信を受ける場合に比べて、格段に短い通話時間で、音楽再生を可能とすることができる。

たとえば、携帯電話機１００および１０２が、ＰＨＳ（Personal Handy

Phone）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ１からユーザ２への一括した情報の移転（移動）や、暗号化したコンテンツデータのみの転送（複製）を行なうことが可能である。

図１に示したような構成においては、暗号化して配信されるコンテンツデータをユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号化キー（鍵）を配送するための方式であり、さらに第２には、配信データを暗号化する方式そのものであり、さらに、第３には、このようにして配信されたデータの無断コピーを防止するためのデータ保護を実現する構成である。

［暗号／復号鍵の構成］

図２は、図１に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

まず、図１に示した構成において、メモリカード１００内のデータ処理を管理するための鍵としては、メモリカードという媒体の種類に固有であり、かつ、メモリカードの種類等を個別に特定するための情報を含む秘密復号鍵Ｋｍｅｄｉａ（ｎ）（ｎ：自然数）と、メモリカードごとに異なる公開暗号化鍵ＫＰｃａｒｄ（ｎ）と、公開暗号化鍵ＫＰｃａｒｄ（ｎ）により暗号化されたデータを復号するための秘密復号鍵Ｋｃａｒｄ（ｎ）とがある。

ここで、鍵Ｋｃａｒｄ（ｎ）や鍵ＫＰｃａｒｄ（ｎ）の表記中の自然数ｎは、各メモリカードを区別するための番号を表わす。

すなわち、公開暗号化鍵ＫＰｃａｒｄ（ｎ）で暗号化されたデータは、各メモリカードごとに存在する秘密復号鍵Ｋｃａｒｄ（ｎ）で復号可能である。したがって、メモリカードにおける配信データの授受にあたっては、基本的には、後に説明するように３つの暗号鍵Ｋｍｅｄｉａ（ｎ）、Ｋｃａｒｄ（ｎ）、ＫＰｃａｒｄ（ｎ）が用いられることになる。

さらに、メモリカード外とメモリカード間でのデータの授受における秘密保持のための暗号鍵としては、各媒体に固有な公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）と、公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）により暗号化されたデータを復号化する

ための秘密復号鍵Ｋｍｅｄｉａ（ｎ）と、各通信ごと、たとえば、音楽サーバ３０へのユーザのアクセスごとに音楽サーバ３０、携帯電話機１００または１０２において生成される共通鍵Ｋｓが用いられる。

ここで、共通鍵Ｋｓは、たとえば、ユーザが音楽サーバ３０に対して１回のアクセスを行なうごとに発生する構成として、１回のアクセスである限り何曲の音楽情報についても同一の共通鍵が用いられる構成としてもよいし、また、たとえば、各曲目ごとにこの共通鍵を変更したうえでその都度ユーザに配信する構成としてもよい。

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、共通鍵Ｋｓを「セッションキー」とも呼ぶことにする。

したがって、共通鍵Ｋｓは各通信セッションに固有の値を有することになり、配信サーバや携帯電話機において管理される。

また、配信されるべきデータについては、まず、暗号化コンテンツデータを復号する鍵であるＫｃ（以下、ライセンスキーと呼ぶ）があり、このライセンスキーＫｃにより暗号化コンテンツデータが復号化されるものとする。さらに、上述したライセンス情報として、当該コンテンツデータを特定できる管理コードや、再生を行なう回数の制限などの情報を含むライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等が存在する。一方、携帯電話は、受信者を識別するためのユーザＩＤデータＵｓｅｒ－ＩＤを保持している。

このような構成とすることで、ライセンスＩＤデータに含まれる情報に応じて、著作権者側の著作権保護に関する制御を行なうことが可能であり、一方ユーザＩＤデータを用いることで、ユーザの個人情報の保護、たとえばユーザのアクセス履歴等が部外者から知ることができないように保護するといったような制御を行なうことが可能である。

配信データにおけるコンテンツデータＤｃは、上述のとおり、たとえば音楽データであり、このコンテンツデータをライセンスキーＫｃで復号化可能なデータを、暗号化コンテンツデータ［Ｄｃ］Ｋｃと呼ぶ。

ここで、［Ｙ］Ｘという表記は、データＹを、キー（鍵）Ｘにより復号可能な暗号に変換したデータであることを示している。なお、暗号化処理、復号処理で

用いられる鍵を、「キー」とも称することとする。

［配信サーバ１０の構成］

図３は、図１に示した配信サーバ１０の構成を示す概略ブロック図である。配信サーバ１０は、コンテンツデータ（音楽データ）を所定の方式に従って暗号化したデータや、ライセンスＩＤ等の配信情報を保持するための配信情報データベース３０４と、各ユーザごとにコンテンツデータへのアクセス回数等に従った課金情報を保持するための課金データベース３０２と、配信情報データベース３０４および課金データベース３０２からのデータをデータバスＢＳ１を介して受取り、所定の暗号化処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

データ処理部３１０は、データバスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１２と、配信制御部３１２に制御されて、セッションキーＫｓを発生するためのセッションキー発生部３１４と、セッションキー発生部３１４より生成されたセッションキーＫｓを、公開暗号化鍵ＫＰｍｅｄｉａにより暗号化して、データバスＢＳ１に与えるための暗号化処理部３１６と、各ユーザの携帯電話機においてセッションキーＫｓにより暗号化されたうえで送信されたデータを通信装置３５０およびデータバスＢＳ１を介して受けて、復号処理を行なう復号処理部３１８と、復号処理部３１８により抽出された公開暗号化鍵ＫＰｃａｒｄ（ｎ）を用いて、ライセンスキーやライセンスＩＤ等のデータを配信制御部３１２に制御されて暗号化するための暗号化処理部３２０と、暗号化処理部３２０の出力を、さらにセッションキーＫｓにより暗号化して、データバスＢＳ１を介して通信装置３５０に与える暗号化処理部３２２とを含む。

［端末（携帯電話機）の構成］

図４は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に

変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのデータバスＢＳ２と、データバスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６と、受信者を識別するためのユーザＩＤデータＵｓｅｒ－ＩＤを保持するユーザＩＤ保持部１１０７と、外部からの指示を携帯電話機１００に与えるためのタッチキー部１１０８と、コントローラ１１０６等から出力される情報をユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データバスＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２と、外部との間でデータの授受を行なうためのコネクタ１１２０と、コネクタ１１２０からのデータをデータバスＢＳ２に与え得る信号に変換し、または、データバスＢＳ２からのデータをコネクタ１１２０に与え得る信号に変換するための外部インタフェース部１１２２とを備える。

ここで、ユーザＩＤデータは、たとえばユーザの電話番号等のデータを含む。

携帯電話機１００は、さらに、音楽サーバ３０からのコンテンツデータを復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とデータバスＢＳ２との間のデータの授受を制御するためのメモリインタフェース１２００と、メモリカード１１０と携帯電話機の他の部分とのデータ授受にあたり、データバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓを乱数等により発生するセッションキー発生部１５０２と、セッションキー発生部１５０２により生成されたセッションキーを暗号化して、データバスＢＳ２に与えるための暗号化処理部１５０４と、セッションキー発生部１５０２において生成された、データバスＢＳ２上のデータをセッションキーＫｓにより復号して出力する復号処理部１５０６と、復号処理部１５０６の出力を受けて、音楽信号を再生するための音楽再生部１５０８と、音楽再生部１５０８の出力と音声再生部１１１２の出力とを受けて、動作モードに応じて選択的に出力するための混合部１５１０と、混合部１５１０の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部１５１２と、デジタルアナログ変換部１５１２の出力を受けて、ヘッドホン１３０と接続するための接続端

子１５１４とを含む。

なお、説明の簡素化のため本発明のコンテンツデータの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

［メモリカードの構成］

図５は、図４に示したメモリカード１１０の構成を説明するための概略ブロック図である。

以下では、端末１００に装着されるメモリカード１１０の公開暗号化鍵ＫＰｍｅｄｉａと、端末１０２に装着されるメモリカード１１２の公開暗号化鍵ＫＰｍｅｄｉａとを区別して、それぞれ、メモリカード１１０に対するものを公開暗号化鍵ＫＰmedia（１）と、メモリカード１１２に対するものを公開暗号化鍵ＫＰmedia（２）と称することにする。

また、これに対応して、公開暗号化鍵ＫＰmedia（１）で暗号化されたデータを復号可能であって、これとは非対称な秘密復号鍵を秘密復号鍵Ｋｍｅｄｉａ（１）と称し、公開暗号化鍵ＫＰmedia（２）で暗号化されたデータを復号可能であって、これとは非対称な秘密復号鍵を秘密復号鍵Ｋｍｅｄｉａ（２）と称することにする。

このように、媒体固有の公開暗号化鍵を区別することにより、以下の説明で明らかとなるように、メモリカードに複数の種類が存在する場合や、より一般的に、メモリカード以外の媒体がシステムのオプションとして存在する場合にも、対応することが可能となる。

メモリカード１１０は、メモリインタフェース１２００との間で信号を端子１２０２を介して授受するデータバスＢＳ３と、公開暗号化鍵ＫＰｍｅｄｉａ（１）の値を保持し、データバスＢＳ３に公開暗号化鍵ＫＰmedia（１）を出力するためのＫＰmedia（１）保持部１４０１と、メモリカード１１０に対応する秘密復号鍵Ｋｍｅｄｉａ（１）を保持するためのＫｍｅｄｉａ（１）保持部１４０２と、データバスＢＳ３にメモリインタフェース１２００から与えられるデータから、秘密復号鍵Ｋｍｅｄｉａ（１）により復号処理をすることにより、セッションキーＫｓを抽出する復号処理部１４０４と、公開暗号化鍵ＫＰｃ

ａｒｄ（１）を保持するためのＫＰｃａｒｄ（１）保持部１４０５と、復号処理部１４０４により抽出されたセッションキーＫｓに基づいて、切換スイッチ１４０８からの出力を暗号化してデータバスＢＳ３に与えるための暗号化処理部１４０６と、データバスＢＳ３上のデータを復号処理部１４０４により抽出されたセッションキーＫｓにより復号処理してデータバスＢＳ４に与えるための復号処理部１４１０と、データバスＢＳ４からメモリカードごとに異なる公開暗号化鍵ＫＰｃａｒｄ（ｎ）で暗号化されているライセンスキーＫｃ、ライセンスＩＤ等のデータを格納し、データバスＢＳ３からライセンスキーＫｃにより暗号化されている暗号化コンテンツデータ［Ｄｃ］Ｋｃを受けて格納するためのメモリ１４１２とを備える。

切換えスイッチ１４０８は、接点Ｐａ、Ｐｂ、Ｐｃを有し、接点ＰａにはＫＰｃａｒｄ（１）保持部１４０５からの公開暗号化鍵ＫＰｃａｒｄ（１）が，接点ＰｂにはデータバスＢＳ５が、接点Ｐｃには暗号化処理部１４１４の出力が与えられる。切換えスイッチ１４０８は、それぞれ、接点Ｐａ、Ｐｂ、Ｐｃに与えられる信号を、動作モードが、「配信モード」、「再生モード」、「移動モード」のいずれであるかに応じて、選択的に暗号化処理部１４０６に与える。

メモリカード１１０は、さらに、秘密復号鍵Ｋｃａｒｄ（１）の値を保持するためのＫｃａｒｄ（１）保持部１４１５と、公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化されており、かつ、メモリ１４１２から読み出されたライセンスキーＫｃ、ライセンスＩＤ等（［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１））を、復号処理してデータバスＢＳ５に与える復号処理部１４１６と、データの移動処理等において、相手先のメモリカードの公開暗号化鍵ＫＰｃａｒｄ（ｎ）を復号処理部１４１０から受けて、この相手方の公開暗号化鍵ＫＰｃａｒｄ（ｎ）に基づいて、データバスＢＳ５上に出力されているライセンスキーＫｃ、ライセンスＩＤ等を暗号化したうえで、切換スイッチ１４０８に出力するための暗号化処理部１４１４と、データバスＢＳ３を介して外部とデータの授受を行い、データバスＢＳ５との間でライセンスＩＤデータ等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０と、データバスＢＳ５との間でライセンスＩＤデータ等のデータの授受が可能なレジスタ１５００とを備える。

なお、図５において実線で囲んだ領域は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読み出しを不能化するためのモジュールＴＲＭに組込まれているものとする。

このようなモジュールは、一般にはタンパーレジスタンスモジュール（Tamper Resistance Module）と呼ばれる。

もちろん、メモリ１４１２も含めて、モジュールＴＲＭ内に組み込まれる構成としてもよい。しかしながら、図５に示したような構成とすることで、メモリ１４１２中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１２中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ１４１２を設ける必要がないので、製造コストが低減されるという利点がある。

図６および図７は、図１および図３～図５で説明したデータ配信システムにおける配信動作を説明するための第１および第２のフローチャートである。

図６および図７においては、ユーザ１が、メモリカード１１０を用いることで、音楽サーバ３０から音楽データの配信を受ける場合の動作を説明している。

まず、ユーザ１の携帯電話機１００から、ユーザによりタッチキー１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

メモリカード１１０においては、この配信リクエストに応じて、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化鍵ＫＰｍｅｄｉａ（１）を音楽サーバ３０に対して送信する（ステップＳ１０２）。

音楽サーバ３０では、メモリカード１１０から転送された配信リクエストならびに公開暗号化鍵ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ１０４）、受信した公開暗号化鍵ＫＰｍｅｄｉａ（１）に基づいて、認証サーバ１２に対して照会を行ない、正規メモリカードからのアクセスの場合は次の処理に移行し（ステップＳ１０６）、正規メモリカードでない場合には、処理を終了する（ステップＳ１５４）。

照会の結果、正規メモリカードであることが確認されると、音楽サーバ３０で

は、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、音楽サーバ３０内の暗号化処理部３１６が、受信した公開暗号化鍵ＫＰｍｅｄｉａ（１）により、このセッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ１０８）。

続いて、音楽サーバ３０は、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３１６からの暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を、通信網を通じて、携帯電話機１００のメモリカード１１０に対して送信する（ステップＳ１１０）。

携帯電話機１００が、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を受信すると（ステップＳ１１２）、メモリカード１１０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、秘密復号鍵Ｋｍｅｄｉａ（１）により復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ１１４）。

続いて、配信動作においては、切換スイッチ１４０８は、接点Ｐａが閉じる状態が選択されているので、暗号化処理部１４０６は、接点Ｐａを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）（メモリカード１１０に対する公開暗号化鍵）を、セッションキーＫｓにより暗号化し（ステップＳ１１６）、データ［ＫＰｃａｒｄ（１）］Ｋｓを生成する（ステップＳ１１８）。

携帯電話機１００は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）］Ｋｓを音楽サーバ３０に対して送信する（ステップＳ１２０）。

音楽サーバ３０では、通信装置３５０によりデータ［ＫＰｃａｒｄ（１）］Ｋｓが受信され（ステップＳ１２２）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、公開暗号化鍵ＫＰｃａｒｄ（１）を復号抽出する（ステップＳ１２４）。

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅ

ｎｓｅを生成する（ステップＳ１２６）。

さらに、音楽サーバ３０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、通信装置３５０を介して、メモリカード１１０に送信する（ステップＳ１２８）。

携帯電話機１００がデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ１３０）、メモリカード１１０においては、受信したデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ１３２）。

一方、音楽サーバ３０は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ１３４）、暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理部３１８より与えられた公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ１３６）。

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらにセッションキーＫｓにより暗号化したデータをデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓをメモリカード１１０に対して送信する。

携帯電話機１００がデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓを受信すると（ステップＳ１４２）、メモリカード１１０においては、復号処理部１４１０がセッションキーＫｓにより復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に記録（格納）する（ステップＳ１４６）。

さらに、メモリカード１１０においては、コントローラ１４２０により制御されて、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅを、レジスタ１５００に格納する（ステップ１４８）。

以上のような動作により、メモリカード自身が、セッションキーＫｓを送る側（音楽サーバ３０）に、公開暗号化鍵ＫＰｍｅｄｉａ（１）を送信した上で、配信を受けることができ、メモリカード１１０が格納するコンテンツデータは再生

可能な状態となる。以下では、メモリカードが格納するコンテンツデータが再生可能な状態となっていることを、「メモリカード１１０は、状態ＳＡにある」と呼ぶことにする。一方、メモリカードが格納するコンテンツデータが再生不可能な状態となっていることを、「メモリカード１１０は、状態ＳＢにある」と呼ぶことにする。

さらに、メモリカード１１０から音楽サーバ３０へは、配信受理が通知され、音楽サーバ３０で配信受理を受信すると（ステップＳ１５０）、課金データベース３０２にユーザ１の課金データが格納され（ステップＳ１５２）、処理が終了する（ステップＳ１５４）。

図８は、携帯電話機１００内において、メモリカード１１０に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図８を参照して、携帯電話機１００のタッチキー部１１０８等からのユーザ１の指示により、再生リクエストがメモリカード１１０に対して出力される（ステップＳ２００）。

メモリカード１１０においては、この再生リクエストに応じて、コントローラ１４２０は、レジスタ１５００に保持されるライセンス情報データＬｉｃｅｎｓｅに基づいて、再生可能なデータに対するリクエストであるかを判断し（ステップＳ２０２）、再生可能と判断した場合は、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化鍵ＫＰｍｅｄｉａ（１）を携帯電話機１００に対して送信する（ステップＳ２０４）。一方、再生不可能と判断した場合は、処理を終了する（ステップＳ２３０）。

再生可能と判断され、メモリカード１１０から公開暗号化鍵ＫＰｍｅｄｉａ（１）が送信された場合、携帯電話機１００では、メモリカード１１０からの公開暗号化鍵ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ２０６）、Ｋｓ発生部１５０２においてセッションキーＫｓを生成し、暗号化処理部１５０４が、公開暗号化鍵ＫＰｍｅｄｉａ（１）により、セッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］ＫＰｍｅｄｉａ（１）を生成し、データバスＢＳ２を介して、メモリカード１１０に対して送信する（ステップＳ２０８）。

メモリカード１１０は、データバスＢＳ２を介して、携帯電話機１００により生成され、かつ暗号化されたセッションキーＫｓを受け取り、秘密復号鍵Ｋｍｅｄｉａ（1）により復号し、セッションキーＫｓを抽出する（ステップＳ２１０）。

続いて、メモリカード１１０は、メモリ１４１２から、暗号化されているデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（1）を読み出し、復号処理部１４１６が復号処理を行なう（ステップＳ２１２）。

秘密復号鍵Ｋｃａｒｄ（1）により、メモリ１４１２から読み出されたデータを復号可能な場合（ステップＳ２１４）、ライセンスキーＫｃが抽出される（ステップＳ２１６）。　一方、再生不可能の場合、処理は終了する（ステップＳ２３２）。

メモリ１４１２から読み出されたデータを再生可能な場合（ステップＳ２１４）は、レジスタ１５００内のライセンス情報データＬｉｃｅｎｓｅのうち、再生回数に関するデータが変更される（ステップＳ２１８）。

続いて、抽出したセッションキーＫｓにより、ライセンスキーＫｃを暗号化し（ステップＳ２２０）、暗号化されたライセンスキー［Ｋｃ］Ｋｓをデータバス ＢＳ２に与える（ステップＳ２２２）。

携帯電話機１００の復号処理部１５０６は、セッションキーＫｓにより復号化処理を行なうことにより、ライセンスキーＫｃを取得する（ステップＳ２２４）。

続いて、メモリカード１１０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読み出し、データバスＢＳ２に与える（ステップＳ２２６）。

携帯電話機１００の音楽再生部１５０８は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたライセンスキーＫｃにより復号処理して平文の音楽データを生成し（ステップＳ２２８）、音楽信号を再生して混合部１５１０に与える（ステップＳ２３０）。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップＳ２３２）。

このような構成とすることで、メモリカード自身が、セッションキーＫｓを送

る側（携帯電話機１００）に、公開暗号化鍵ＫＰｍｅｄｉａ（1）を送信した上で、再生動作を行なうことが可能となる。

図９および図１０は、２つのメモリカード間において、音楽データおよびキーデータ等の移動または複製を行なう処理を説明するための第１および第２のフローチャートである。

まず、携帯電話機１０２が送信側であり、携帯電話機１００が受信側であるものとする。また、携帯電話機１０2にも、メモリカード１１０と同様の構成を有するメモリカード１１２が装着されているものとする。

携帯電話機１０２は、まず、自身の側のメモリカード１１２および携帯電話機１００に対して、移動リクエストまたは複製リクエストを出力する（ステップＳ３００）。

メモリカード１１２は、これに応じて、メモリ１４１２内の暗号化コンテンツデータ［Ｄｃ］Ｋｃを読み出して、メモリカード１１０に対して出力し（ステップＳ３０２）、一方、携帯電話機１００は、携帯電話機１０２からリクエストを受信して（ステップＳ３０１）、メモリカード１１０では、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２に格納する（ステップＳ３０４）。

続いて、携帯電話機１０２および１００においては、ステップＳ３００において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップＳ３０６、ステップＳ３０６´）、「移動リクエスト」である場合、メモリカード１１２は、公開暗号化鍵ＫＰｍｅｄｉａ（2）を携帯電話機１０２に対して送信し（ステップＳ３０８）、携帯電話機１０２は、公開暗号化鍵ＫＰｍｅｄｉａ（2）を受信する（ステップＳ３１２）。一方、メモリカード１１０は、「移動リクエスト」である場合、公開暗号化鍵ＫＰｍｅｄｉａ（1）を携帯電話機１００に出力し（ステップＳ３０８´）、携帯電話機１００は、公開暗号化鍵ＫＰｍｅｄｉａ（1）を携帯電話機１０２に対して送信する（ステップＳ３１０）。

携帯電話機１０２が、公開暗号化鍵ＫＰｍｅｄｉａ（1）および公開暗号化鍵ＫＰｍｅｄｉａ（2）を受信すると（ステップＳ３１２、ステップＳ３１２´）、携帯電話機１０２においては、セッションキー発生回路１５０２は、セッ

ションキーＫｓを生成し（ステップＳ３０３）、公開暗号化鍵ＫＰｍｅｄｉａ（１）および公開暗号化鍵ＫＰmedia（２）を用いて、暗号化処理部１５０４がセッションキーＫｓを暗号化する（ステップＳ３１４）。

携帯電話機１０２は、データバスＢＳ２を介して、メモリカード１１２に対しては暗号化セッションキー［Ｋｓ］ＫＰｍｅｄｉａ（２）を伝達し、メモリカード１１２においては、秘密復号鍵Ｋｍｅｄｉａ（２）によりセッションキーＫｓを復号抽出する（ステップＳ３２８）。

さらに、携帯電話機１０２は、暗号化セッションキー［Ｋｓ］ＫＰｍｅｄｉａ（１）を携帯電話機１００に対して送信する（ステップＳ３１６）。携帯電話機１００は、暗号化セッションキー［Ｋｓ］ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ３１８）、メモリカード１１０に伝達し、メモリカード１１０は、復号処理部１４０４が復号して、セッションキーＫｓを受理する（ステップＳ３２０）。

メモリカード１１０においては、セッションキーＫｓによりメモリカード１１０の公開暗号化鍵ＫＰｃａｒｄ（１）を暗号化して（ステップＳ３２２）、携帯電話機１００から携帯電話機１０２に対して暗号化されたデータ［ＫＰｃａｒｄ（１）］Ｋｓを送信する（ステップＳ３２４）。携帯電話機１０２は、データ［ＫＰｃａｒｄ（１）］Ｋｓを受信し（ステップＳ３２６）、かつ、メモリカード１１２によるセッションキーＫｓの受理が完了すると（ステップＳ３２８）、メモリカード１１２においては、メモリカード１１０から送信された暗号化データ［ＫＰｃａｒｄ（１）］Ｋｓをセッションキーによりｓ復号化して、メモリカード１１０の公開暗号化鍵ＫＰｃａｒｄ（１）を復号抽出する（ステップＳ３３０）。

続いて、メモリカード１１２においては、メモリ１４１２からメモリカード１１２の公開暗号化鍵ＫＰｃａｒｄ（２）により暗号化されているライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅが読み出される（ステップＳ３３２）。

続いて、メモリカード１１２の復号処理部１４１６が、秘密復号鍵Ｋｃａｒｄ（２）により、ライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅを復

号処理する（ステップＳ３３４）。

メモリカード１１２のコントローラ１４２０は、このようにして復号されたライセンス情報データＬｉｃｅｎｓｅの値を、レジスタ１５００内のデータ値と置換する（ステップＳ３３６）。

さらに、メモリカード１１２の暗号化処理部１４１４は、復号処理部１４１０において抽出されたメモリカード１１０における公開暗号化鍵ＫＰｃａｒｄ（1）により、ライセンスキーK,c、ライセンス情報データＬｉｃｅｎｓｅとを暗号化する（ステップＳ３３８）。

メモリカード１１２の暗号化処理部１４１４により暗号化されたデータは、切換スイッチ１４０８（接点Ｐｃが閉じている）を介して、さらに、暗号化処理部１４０６に与えられ、暗号化処理部１４０６は、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（1）をセッションキーＫｓにより暗号化してデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（1）］Ｋｓを生成する（ステップＳ３４０）。

続いて、メモリカード１１２は、携帯電話機１０２に対してデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（1）］Ｋｓを出力し（ステップＳ３４２）、携帯電話機１０２はデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（1）］Ｋｓを携帯電話機１００に対して送信する（ステップＳ３４４）。

携帯電話機１００が受信したデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（1）］Ｋｓは（ステップＳ３４６）、メモリカード１１０に対して伝達され、メモリカード１１０の復号処理部１４１０は、暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（1）］Ｋｓを復号して、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（1）を受理する（ステップＳ３４８）。

メモリカード１１０においては、復号処理部１４１０により、セッションキーＫｓに基づいて復号化処理されたデータをメモリ１４１２に記録する（ステップＳ３５０）。さらに、メモリカード１１０においては、復号処理部１４１６が、秘密復号鍵Ｋｃａｒｄ（1）に基づいて、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（1）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅをレジスタ１５００に格納する（ステップＳ３５２）。

復号されたライセンス情報データＬｉｃｅｎｓｅのレジスタ１５００への格納

が終了すると、メモリカード１１０は携帯電話機１００に移動受理を通知し、携帯電話機１００は、携帯電話機１０２に対して移動受理を送信する（ステップＳ３５４）。

携帯電話機１０２は、携帯電話機１００からの移動受理を受信すると、メモリカード１１２に対してこれを転送し、メモリカード１１２は、これに応じて、レジスタ１５００に格納されたライセンス情報データＬｉｃｅｎｓｅを消去する（ステップ３５８）。

一方、携帯電話機１０２では、移動受理が受信されたことに応じて、ディスプレイ１１１０上に、ユーザ２に対して、メモリカード１１２のメモリ１４１２内に格納されている移動データに対応する記憶データの消去を行なって良いかを問うメッセージを表示する。これに応じて、ユーザ２は、タッチキー１１０８からこのメッセージに対する回答を入力する（ステップＳ３６０）。

レジスタ１５００内のデータの消去が完了し（ステップＳ３５８）、かつ、上記メッセージに対する回答の入力が行なわれると（ステップＳ３６０）、メモリカード１１２内のコントローラ１４２０は、メモリ１４１２内のデータの消去を行なうかの判断を行なう（ステップＳ３６２）。

メモリ１４１２内の該当データの消去が指示されている場合（ステップＳ３６２）、コントローラ１４２０により制御されて、メモリ１４１２内の暗号化コンテンツデータ［Ｄｃ］Ｋｃおよびデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（２）が消去され（ステップＳ３６４）、処理が終了する（ステップＳ３７４）。

一方、メモリ１４１２内の該当データの消去が指示されていない場合（ステップＳ３６２）、処理は終了する（ステップＳ３７４）。この場合、メモリ１４１２内には、暗号化コンテンツデータ［Ｄｃ］Ｋｃおよびデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（２）が残っていることになるが、レジスタ１５００内にライセンス情報データＬｉｃｅｎｓｅが存在しないため、ユーザ２は、再度、音楽サーバ３０から再生情報を配信してもらわない限り、音楽データの再生を行なうことはできない。すなわち、メモリカード１１２は「状態ＳＢ」となる。メモリカード１１０においては、暗号化コンテンツデータ以外にも、ライセンスキーＫ

c、ライセンス情報データが移動されているので、メモリカード１１０は「状態ＳＡ」となっている。

一方、ステップＳ３０６´において、「複製リクエスト」が与えられていると判断された場合は、携帯電話機１００から携帯電話機１０２に対して複製受理が送信される（ステップＳ３７０）。携帯電話機１０２において、複製受理を受信すると（ステップＳ３７２）、処理が終了する（ステップＳ３７４）。

このような構成とすることで、メモリカード自身が、セッションキーＫｓを送る側（携帯電話機１００）に、公開暗号化鍵ＫＰｍｅｄｉａ（１）およびＫＰｍｅｄｉａ（２）を送信した上で、移動動作を行なうこと、および複製動作を行なうことが可能となる。

［実施の形態２］

実施の形態２のデータ配信システムにおいては、実施の形態１のデータ配信システムの構成と異なって、配信サーバ、携帯電話機およびメモリカードの各々が、独自のセッションキーを生成する構成となっていることを１つの特徴とする。すなわち、配信サーバまたは携帯電話機の発生するセッションキーをセッションキーＫｓとし、一方のメモリカード１２０の発生するセッションキーをセッションキーＫｓ１とし、メモリカード１２０と同様の構成を有する他方のメモリカード１２２の発生するセッションキーをセッションキーＫｓ２とする。

すなわち、実施の形態２のデータ配信システムにおいては、システムを構成する機器の各々が、自身でセッションキーを生成し、データを受け取るとき、言い換えるとデータの送信先になっている場合には、相手方（送信元）に対して、まず、セッションキーを配送する。送信元は、この送信先から配送されたセッションキーでデータを暗号化し、この暗号化データを送信する。送信先では、自身で生成したセッションキーにより、受け取ったデータを復号化するという構成を１つの特徴とするものである。

また、上記のような動作を実現するために、再生動作において、携帯電話機側がメモリカードの生成するセッションキーを受け取るための公開暗号化鍵をＫＰｐとし、この公開暗号化鍵ＫＰｐで暗号化されたデータを復号化できる秘密復号鍵を鍵Ｋｐとする。

図１１は、実施の形態２のメモリカード１２０に対応した配信サーバ１１の構成を示す概略ブロック図である。図３に示した配信サーバ１０の構成と異なる点は、データ処理部３１０における暗号化処理部３２２は、Ｋｓ発生部３１４からのセッションキーＫｓに基づいてではなく、携帯電話機に装着されたメモリカードからセッションキーＫｓ１、Ｋｓ２により暗号化されて送信され、復号処理部３１８により復号抽出されたセッションキー、たとえば、セッションキーＫｓ１に基づいて、暗号化処理部３２０の出力をさらに暗号化して、データバスＢＳ１を介して通信装置３５０に与える点である。

配信サーバ１１のその他の点は、図３に示した実施の形態１の配信サーバ１０の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図１２は、実施の形態２における携帯電話機１０１の構成を説明するための概略ブロック図である。

図４に示した携帯電話機１００の構成と異なる点は、まず、メモリカード１２０が装着されていること以外に、携帯電話機１０１は、公開暗号化鍵ＫＰｐを保持して、再生動作時に公開暗号化鍵ＫＰｐをデータバスＢＳ２に出力するＫＰｐ保持部１５２４を備える構成となっていることである。

さらに、携帯電話機１０１は、秘密復号鍵Ｋｐを保持するＫｐ保持部１５２０と、このＫｐ保持部１５２０から与えられる秘密復号鍵Ｋｐに基づいて、データバスＢＳ２を介してメモリカード１２０から与えられる公開暗号化鍵ＫＰｐで暗号化されたセッションキーＫｓ１を復号し抽出する復号処理部１５２２とをさらに備える構成となっている。しかも、暗号化処理部１５０４は、この復号処理部１５２２から与えられるセッションキーＫｓ１により、Ｋｓ発生部１５０２からの自身のセッションキーＫｓを暗号化してデータバスＢＳ２に出力する。

携帯電話機１０１のその他の点は、図４に示した実施の形態１の携帯電話機１００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図１３は、本発明の実施の形態２のメモリカード１２０の構成を説明するための概略ブロック図であり、実施の形態１の図５と対比される図である。

メモリカード１２０の構成が、メモリカード１１０の構成と異なる点は、まず、メモリカード１２０は、このカード独自のセッションキーＫｓ１を発生するセッションキーＫｓ１発生部１４３２を備えることである。

さらに、メモリカード１２０は、セッションキー発生回路１４３２で生成されたセッションキーＫｓ１を、暗号化してデータバスＢＳ３に与えるための暗号化処理部１４３０を備える。

これに応じて、メモリカード１２０は、さらに、再生モードにおいて、形態電話機１０１の公開暗号化鍵ＫＰｐを受けて保持するＫＰｐ受理部１４０７と、移動モードにおいて、相手方（移動先）の公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）を受けて保持するＫＰｍｅｄｉａ受理部１４０３と、このＫＰｍｅｄｉａ受理部１４０３の出力とＫＰｐ受理部１４０７の出力とを受けて、動作モードに応じていずれか一方を出力する切換えスイッチ１４３６を備える。切換えスイッチ１４３６は、接点ＰｉおよびＰｈとを有し、接点ＰｉはＫＰｐ受理部１４０７と、接点ＰｈはＫＰｍｅｄｉａ受理部１４０３とそれぞれ結合する。暗号化処理部１４３０は、切換えスイッチ１４３６から与えられる公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）または公開暗号化鍵ＫＰｐのいずれかにより、Ｋｓ１発生部１４３２からのセッションキーＫｓ１を暗号化して、データバスＢＳ３に与える。

すなわち、切換えスイッチ１４３６は、配信動作のとき、および移動動作において移動先となっているときは、未使用状態であり、再生動作の時は、接点Ｐｉの側に閉じており、移動動作において移動元となっているときは、接点Ｐｈの側に閉じている。

メモリカード１２０は、さらに、接点Ｐｅ、ＰｆおよびＰｇを有し、復号処理部１４０４から与えられる音楽サーバからのセッションキーＫｓと、Ｋｓ１発生部１４３２の出力と、データバスＢＳ４から与えられる携帯電話機１０１からのセッションキーＫｓとを受けて、動作モードに応じていずれか１つを選択的に出力する切換えスイッチ１４３５を備える。接点Ｐｅには復号処理部１４０４からの出力が、接点ＰｆにはＫｓ１発生部１４３２の出力が、接点Ｐｇにはデータバスバス４がそれぞれ結合している。したがって、暗号化処理部１４０６と復号処理部１４１０は、この切換えスイッチ１４３５から与えられるキーに基づいて、

それぞれ、暗号化処理および復号処理を行なう。

すなわち、切換えスイッチ１４３５は、配信動作の場合に音楽サーバ３１からのセッションキーＫｓ１の抽出を行なうときは、接点Ｐｅの側に閉じており、配信動作の場合に音楽サーバ３１からの暗号化されたライセンスキーＫｃ、ライセンス情報データについてセッションキーＫｓ１による復号を行なうときは、接点Ｐｆの側に閉じている。切換えスイッチ１４３５は、再生動作において復号処理を行なうときは、接点Ｐｆの側に閉じており、再生動作において暗号化処理を行なうときは、接点Ｐｇの側に閉じている。切換えスイッチ１４３５は、移動動作において移動元となっている場合に復号処理を行なうときは、接点Ｐｆの側に閉じており、移動動作において移動元となっている場合に暗号化処理を行なうときは、接点Ｐｇの側に閉じている。切換えスイッチ１４３５は、移動動作において移動先となっている場合に移動元のセッションキーを受け取るときは、接点Ｐｅの側に閉じており、移動動作において移動先となっている場合にライセンスキーＫｃおよびライセンス情報データＬｉｃｅｎｓｅを受け取るときは、接点Ｐｆの側に閉じている。

メモリカード１２０は、さらに、接点Ｐａ、Ｐｂ、ＰｃおよびＰｄ を有し、Ｋｓ１発生部１４３２から与えられる自身のセッションキーＫｓ１と、ＫＰｃａｒｄ保持部１４０５の出力と、データバスＢＳ５から与えられるライセンスキーＫｃと、暗号化処理部１４１４から与えられ、相手方の公開暗号化鍵ＫＰｃａｒｄ（ｎ）により暗号化されたライセンスキーＫｃおよびライセンス情報データＬｉｃｅｎｓｅを受けて、動作モードに応じていずれか１つを選択的に出力する切換えスイッチ１４０９を、切換えスイッチ１４０８の替わりに備える。

接点ＰａにはＫｓ１発生部１４３２からの出力が、接点ＰｂにはＫＰｃａｒｄ（１）保持部１４０５の出力が、接点ＰｃにはデータバスＢＳ５が、接点Ｐｄには暗号化処理部１４１４の出力が、それぞれ結合している。したがって、暗号化処理部１４０６は、この切換えスイッチ１４０９から与えられるデータに対して、それぞれ、暗号化処理を行なう。

すなわち、切換えスイッチ１４０９は、配信モードにおいて、配信先となっている場合に音楽サーバ３１に自身の公開暗号化鍵ＫＰｃａｒｄ（１）や自身のセ

ッションキーＫｓ１を送信するときは、順次、接点Ｐｂの側および接点Ｐａの側に閉じる。切換えスイッチ１４０９は、再生モードのときは、接点Ｐｃの側に閉じており、移動モードにおいて移動元となっているときは、接点Ｐｄの側に閉じている。切換えスイッチ１４０９は、移動モードにおいて移動先となっている場合にも移動元に自身の公開暗号化鍵ＫＰｃａｒｄ（１）や自身のセッションキーＫｓ１を送信するときは、順次、接点Ｐｂの側および接点Ｐａの側に閉じる。

図１４および図１５は、図１３で説明したメモリカード１２０を用いた配信モードを説明するための第１および第２のフローチャートである。

図１４および図１５においても、ユーザ１が、メモリカード１２０を用いることで、音楽サーバ３１から音楽データの配信を受ける配信モードの動作を説明している。

まず、ユーザ１の携帯電話機１０１から、ユーザによりタッチキー１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

メモリカード１２０においては、この配信リクエストに応じて、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化鍵ＫＰｍｅｄｉａ（１）を音楽サーバ３１に対して送信する（ステップＳ１０２）。さらに、メモリカード１２０においては、Ｋｓ１発生部１４３２によりセッションキーＫｓ１が生成される（ステップＳ１０９）。

音楽サーバ３１では、メモリカード１２０から転送された配信リクエストならびに公開暗号化鍵ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ１０４）、受信した公開暗号化鍵ＫＰｍｅｄｉａ（１）に基づいて、認証サーバ１２に対して照会を行ない、正規のメモリカードを用いたアクセスの場合は次の処理に移行し（ステップＳ１０６）、正規のメモリカードでない場合には、処理を終了する（ステップＳ１５４）。

照会の結果、正規のメモリカードであることが確認されると、音楽サーバ３１では、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、音楽サーバ３１内の暗号化処理部３１６が、受信した公開暗号化鍵ＫＰｍｅｄｉａ（１）により、このセッションキーＫｓを暗号化して暗号化セッションキ

ー［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ１０８）。

続いて、音楽サーバ３１は、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３１６からの暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を、通信網を通じて、携帯電話機１０１のメモリカード１２０に対して送信する（ステップＳ１１０）。

携帯電話機１０１が、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を受信すると（ステップＳ１１２）、メモリカード１２０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、秘密復号鍵Ｋｍｅｄｉａ（１）で復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ１１４）。

続いて、配信モードにおいては、切換えスイッチ１４０９は、接点ＰａまたはＰｂが順次閉じる状態が選択されるので、暗号化処理部１４０６は、接点Ｐａを介してセッションキー発生部１４３２から与えられるセッションキーＫｓ１と接点Ｐｂを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）（メモリカード１２０に対する公開暗号化鍵）とを、セッションキーＫｓにより暗号化し（ステップＳ１１６）、データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを生成する（ステップＳ１１８）。

携帯電話機１０１は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを音楽サーバ３１に対して送信する（ステップＳ１２０）。

音楽サーバ３１では、通信装置３５０によりデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓが受信され（ステップＳ１２２）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ１を復号抽出する（ステップＳ１２４）。

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ１２６）。

さらに、音楽サーバ３１は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報

データベース３０４より取得して、通信装置３５０を介して、メモリカード１２０に送信する（ステップＳ１２８）。

携帯電話機１０１が暗号化コンテンツデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ１３０）、メモリカード１２０においては、受信した暗号化コンテンツデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ１３２）。

一方、音楽サーバ３１は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ１３４）、暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理部３１８より与えられた公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ１３６）。

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらに、メモリカード１２０からのセッションキーＫｓ１により暗号化したデータをデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１をメモリカード１２０に対して送信する。

携帯電話機１０１がデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を受信すると（ステップＳ１４２）、メモリカード１２０においては、復号処理部１４１０が接点Ｐｆを介してＫｓ１発生部１４３２から与えられるセッションキーＫｓ１により復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に格納する（ステップＳ１４６）。

さらに、メモリカード１２０においては、コントローラ１４２０により制御されて、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅを、レジスタ１５００に格納する（ステップ１４８）。

以上のような動作により、メモリカード１２０自身が、暗号化コンテンツデータを送る側（音楽サーバ３１）に、公開暗号化鍵ＫＰｍｅｄｉａ（１）およびセッションキーＫｓ１を送信した上で、配信を受けることができ、メモリカード１２０は、音楽情報を再生可能な状態となる。

さらに、メモリカード１２０から音楽サーバ３１へは、配信受理が通知され、音楽サーバ３１で配信受理を受信すると（ステップＳ１５０）、課金データベース３０２にユーザ１の課金データが格納され（ステップＳ１５２）、処理が終了する（ステップＳ１５４）。

図１６および図１７は、携帯電話機１０１内において、メモリカード１２０に保持された暗号化コンテンツデータから、音楽データであるコンテンツデータを復号化し、音楽として外部に出力するための再生モードを説明する第１および第２のフローチャートである。

図１６および図１７を参照して、携帯電話機のタッチキー１１０８等からのユーザ１の指示により、再生リクエストがメモリカード１２０に対して出力される（ステップＳ２００）。

メモリカード１２０においては、この再生リクエストに応じて、コントローラ１４２０は、レジスタ１５００に保持されるライセンス情報データＬｉｃｅｎｓｅに基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップＳ２０２）、再生可能と判断した場合は、再生可能通知を携帯電話機１０１に対して送信する（ステップＳ２４０）。一方、再生不可能と判断した場合は、処理を終了する（ステップＳ２８０）。

再生可能と判断され、メモリカード１２０から再生可能通知が送信された場合、携帯電話機１０１では、公開暗号化鍵ＫＰｐをメモリカード１２０に送信し（ステップＳ２４２）、Ｋｓ発生部１５０２においてセッションキーＫｓを生成する（ステップＳ２４４）。

一方、メモリカード１２０も、セッションキーＫｓ１を生成する（ステップＳ２４０）。メモリカード１２０は、さらに、データバスＢＳ２を介して携帯電話機１０１から受けとった公開暗号化鍵ＫＰｐによりセッションキーＫｓ１を暗合化し（ステップＳ２４８）、生成された暗号化セッションキー［Ｋｓ１］Ｋｐを携帯電話機１０１に対して送信する（ステップＳ２５０）。

携帯電話機１０１では、メモリカード１２０からの暗号化セッションキー［Ｋｓ１］Ｋｐを受信すると、復号処理部１５２２が、秘密復号鍵Ｋｐにより復号化してメモリカード１２０で生成したセッションキーＫｓ１を抽出する（ステップ

Ｓ２５２）。続いて、携帯電話機１０１の暗号化処理部１５０４は、携帯電話機１０１で生成したセッションキーＫｓをセッションキーＫｓ１により暗号化して、暗号化セッションキー［Ｋｓ］Ｋｓ１を生成し（ステップＳ２５４）、この暗号化セッションキー［Ｋｓ］Ｋｓ１をメモリカード１２０に対して送信する（ステップＳ２５６）。

メモリカード１２０は、データバスＢＳ２を介して、携帯電話機１０１により生成された暗号化セッションキー［Ｋｓ］Ｋｓ１を受け取り、セッションキーＫｓ１により復号し、携帯電話機１０１で生成したセッションキーＫｓを抽出する（ステップＳ２５８）。

続いて、メモリカード１２０は、メモリ１４１２から、暗号化されているデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を読み出し、復号処理部１４１６が復号処理を行なう（ステップＳ２６０）。

秘密復号鍵Ｋｃａｒｄ（１）により、メモリ１４１２から読み出されたデータを復号可能な場合（ステップＳ２６２）、ライセンスキーＫｃが抽出される（ステップＳ２６４）。一方、復号不可能の場合、処理は終了する（ステップＳ２８０）。

メモリ１４１２から読み出されたデータを復号可能な場合は、さらに、レジスタ１５００内のライセンス情報データＬｉｃｅｎｓｅのうち、再生回数に関するデータが変更される（ステップＳ２６６）。

続いて、メモリカード１２０においては、暗号化処理部１４０６が、抽出したセッションキーＫｓにより、ライセンスキーＫｃを暗号化し（ステップＳ２６８）、暗号化ライセンスキー［Ｋｃ］Ｋｓをデータバスバス２に与える（ステップＳ２７０）。

携帯電話機１０１の復号処理部１５０６は、セッションキーＫｓにより復号化処理を行なうことにより、ライセンスキーＫｃを取得する（ステップＳ２７２）。

続いて、メモリカード１２０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読み出し、データバスＢＳ２に与える（ステップＳ２７４）。

携帯電話機１０１の音楽再生部１５０８は、暗号化コンテンツデータ［Ｄｃ］

Ｋｃを、抽出されたライセンスキーＫｃにより復号処理して平文のコンテンツデータを生成し（ステップＳ２７６）、音楽信号を再生して混合部１５１０に与える（ステップＳ２７６）。デジタルアナログ変換部１５１２は、混合部１５１０からの音楽信号を受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップＳ２３２）。

このような構成とすることで、メモリカード自身および携帯電話自身が、それぞれセッションキーＫｓ１またはＫｓを生成し、これにより暗号化されたデータの授受を行なった上で、再生動作を行なうことが可能となる。

図１８および図１９は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動モードまたは複製モードを行なう処理を説明するための第１および第２のフローチャートである。

まず、携帯電話機１０１と同様の構成を有する携帯電話機１０３が送信側であり、携帯電話機１０１が受信側であるものとする。また、携帯電話機１０３にも、メモリカード１２０と同様の構成を有するメモリカード１２２が装着されているものとする。

携帯電話機１０３は、まず、自身の側のメモリカード１２２および携帯電話機１０１に対して、移動リクエストまたは複製リクエストを出力する（ステップＳ３００）。

メモリカード１２２は、これに応じて、メモリ１４１２内の暗号化コンテンツデータ［Ｄｃ］Ｋｃを読み出して、メモリカード１２０に対して出力し（ステップＳ３０２）、一方、携帯電話機１０１は、携帯電話機１０３からのリクエストを受信し（ステップＳ３０１）、メモリカード１２０では、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２に格納する（ステップＳ３０４）。

続いて、携帯電話機１０３および１０１においては、ステップＳ３００において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップＳ３０６、ステップＳ３０６´）、「移動リクエスト」である場合、メモリカード１２０は、公開暗号化鍵ＫＰｍｅｄｉａ（１）を携帯電話機１０１に出力し（ステップＳ３０８）、携帯電話機１０１は、公開暗号化鍵ＫＰｍｅｄｉａ（１）を携帯電話機１０３に対して送信する（ステップＳ

３１０）。

携帯電話機１０３が、公開暗号化鍵ＫＰｍｅｄｉａ（１）を受信し（ステップＳ３１２）、メモリカード１２２に転送すると（ステップＳ３１３）、メモリカード１２２のＫｓ２発生回路１４３２は、セッションキーＫｓ２を生成し（ステップＳ３１４）、公開暗号化鍵ＫＰｍｅｄｉａ（１）を用いて、暗号化処理部１４３０がセッションキーＫｓ２を暗号化する（ステップＳ３１５）。

携帯電話機１０３は、暗号化セッションキー［Ｋｓ２］ＫＰｍｅｄｉａ（１）を携帯電話機１０１に対して送信する（ステップＳ３１６）。携帯電話機１０１は、暗号化セッションキー［Ｋｓ２］ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ３１８）、メモリカード１２０に伝達し、メモリカード１２０は、復号処理部１４０４が復号して、セッションキーＫｓ２を受理し、さらに、セッションキー生成部１４３２で、メモリカード１２０におけるセッションキーＫｓ１が生成される（ステップＳ３２０）。

メモリカード１２０においては、セッションキーＫｓ２によりメモリカード１２０の公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ１を暗号化して（ステップＳ３２２）、携帯電話機１０１から携帯電話機１０３に対して暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓ２を送信する（ステップＳ３２４）。携帯電話機１０３は、データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓ２を受信し（ステップＳ３２６）、メモリカード１２２に転送する。

メモリカード１２２においては、復号処理部１４１０が、メモリカード１２０から送信された暗号化データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓ２をセッションキーＫｓ２により復号化して、メモリカード１２０の公開暗号化鍵ＫＰｃａｒｄ（１）、セッションキーＫｓ１を復号抽出する（ステップＳ３３０）。

続いて、メモリカード１２２においては、メモリ１４１２からメモリカード１２２の公開暗号化鍵ＫＰｃａｒｄ（２）により暗号化されているライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅに対応する［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（２）が読み出される（ステップＳ３３２）。

続いて、メモリカード１２２の復号処理部１４１６が、秘密復号鍵Ｋｃａｒｄ（２）により、［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（２）を復号処理する（ス

テップＳ３３４）。

メモリカード１２２のコントローラ１４２０は、このようにして復号されたライセンス情報データＬｉｃｅｎｓｅの値を、レジスタ１５００内のデータ値と置換する（ステップＳ３３６）。

さらに、メモリカード１２２の暗号化処理部１４１４は、復号処理部１４１０において抽出されたメモリカード１２０における公開暗号化鍵ＫＰｃａｒｄ（１）により、ライセンスキーKc、ライセンス情報データＬｉｃｅｎｓｅとを暗号化する（ステップＳ３３８）。

メモリカード１２２の暗号化処理部１４１４により暗号化されたデータは、切換えスイッチ１４０９（接点Ｐｄが閉じている）を介して、さらに、暗号化処理部１４０６に与えられ、メモリカード１２２の暗号化処理部１４０６は、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）をセッションキーＫｓ１により暗号化してデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を生成する（ステップＳ３４０）。

続いて、メモリカード１２２は、携帯電話機１０３に対してデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を出力し（ステップＳ３４２）、携帯電話機１０３はデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を携帯電話機１０１に対して送信する（ステップＳ３４４）。

携帯電話機１０１が受信したデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１は（ステップＳ３４６）、メモリカード１２０に対して伝達され、メモリカード１２０の復号処理部１４１０は、暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を復号して、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受理する（ステップＳ３４８）。

メモリカード１２０においては、復号処理部１４１０により、セッションキーＫｓ１に基づいて復号化処理されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）をメモリ１４１２に格納する（ステップＳ３５０）。さらに、メモリカード１２０においては、復号処理部１４１６が、秘密復号鍵Ｋｃａｒｄ（１）に基づいて、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅをレジスタ１５００に格納する（ステッ

プＳ３５２）。

以後の移動モードにおける処理ならびに複製モードにおけるメモリカード１２０および１２２の処理は、図９および図１０で説明した実施の形態１のメモリカード１１０、１１２等の処理と同様であるので、その説明は繰り返さない。

このような構成とすることで、移動元および移動先のメモリカード自身が、セッションキーをそれぞれ生成した上で、移動モードを行なうが可能となる。

したがって、データバス上等で伝達されるデータのライセンスキーＫｃおよびライセンス情報データＬｉｃｅｎｓｅを暗号化する鍵が、セッションごとに、かつ、機器ごとに変更されるので、ライセンスキーＫｃおよびライセンス情報データＬｉｃｅｎｓｅの授受のセキュリティが一層向上するという効果がある。

しかも、以上のような構成を用いることで、たとえば、メモリカード１２２からメモリカード１２０へのデータの移動を、上述したようなセッションキー発生回路１５０２を有する携帯電話端末を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

ここで、移動時には、再生回数を制限するライセンス情報データ内の設定については、メモリ１４１２に記録されたライセンス情報データを、レジスタ１５００にて再生の都度修正された再生回数を記録したライセンス情報データに変更することで、ライセンス情報データを更新する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

［実施の形態３］

実施の形態３のデータ配信システムにおいては、ユーザは、配信キャリアである携帯電話会社から暗号化コンテンツデータの配信を受けるのではなく、たとえば、街頭などに設置されているコンテンツデータ販売機から暗号化コンテンツデータの供給を受ける構成となっていることを１つの特徴とする。

図２０は、このような実施の形態３のデータ配信システムの構成を説明するための概念図である。なお、携帯電話機１００およびメモリカード１１０の構成は

実施の形態１で説明したものと同様であるので、その説明は繰り返さない。

図２０を参照して、コンテンツデータ販売機２０００は、ユーザに対して配信作業における案内等を出力するためのディスプレイ２００２と、ユーザから指示を入力するためのキーボード２００４と、料金投入口２００６と、携帯電話機１００とコネクタ１１２０を介してデータの授受を行なうための外部コネクタ２０１０とを備える。さらに、コンテンツデータ販売機２０００は、携帯電話網等の通信路を介して、販売記録等を管理するための管理サーバ２２００と接続している。

図２１は、実施の形態３のコンテンツデータ販売機２０００の構成を示す概略ブロック図である。コンテンツデータ販売機２０００は、上述したように、ディスプレイ２００２と、キーボード２００４と、料金投入口２００６からの投入金を受ける料金受理部２０２０と、外部コネクタ２０１０と、コネクタ２０１０とデータバスとの間に設けられるインタフェース部２０１２と、コンテンツデータ（音楽データ）を所定の方式に従って暗号化したデータや、ライセンス情報データ等の配信情報を保持するための配信情報データベース３０４と、管理サーバ２２００との間で情報の授受をするための通信装置３６０と、配信情報データベース３０４および管理サーバ２２００からのデータをデータバスＢＳ１を介して受取り、所定の暗号化処理を行なうためのデータ処理部２１００とを備える。

データ処理部２１００中は、実施の形態１と同様に、データバスＢＳ１上のデータに応じて、データ処理部２１００の動作を制御するための配信制御部３１２と、配信制御部３１２に制御されて、セッションキーＫｓを発生するためのセッションキー発生部３１４と、セッションキー発生部３１４より生成されたセッションキーＫｓを、カード媒体に固有な公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）により暗号化して、データバスＢＳ１に与えるための暗号化処理部３１６と、各ユーザの携帯電話機においてセッションキーＫｓにより暗号化されたうえでコネクタ２０１０から与えられたデータをデータバスＢＳ１を介して受けて、復号処理を行なう復号処理部３１８と、復号処理部３１８により抽出された公開暗号化鍵ＫＰｃａｒｄ（ｎ）を用いて、ライセンス情報データを配信制御部３１２に制御されて暗号化するための暗号化処理部３２０と、暗号化処理部３２０の出力を、さら

にセッションキーＫｓにより暗号化して、データバスＢＳ１を介してコネクタ２０１０に与える暗号化処理部３２２とを含む。

図２２および図２３は、図２０および図２１で説明したデータ配信システムにおける配信モードを説明するための第１および第２のフローチャートである。

図２２および図２３においては、ユーザ１が、メモリカード１１０を用いることで、コンテンツデータ販売機２０００から音楽データの配信を受ける場合の動作を説明している。

まず、ユーザが、コンテンツデータ販売機２０００のキーボード２００４のキーボタンの操作等によって、配信リクエストを指示する（ステップＳ４００）。コンテンツデータ販売機２０００は、メモリカード１１０に対して公開暗号化鍵ＫＰｍｅｄｉａ（１）の送信依頼を出力する（ステップＳ４０２）。

メモリカード１１０においては、この公開暗号化鍵ＫＰｍｅｄｉａ（１）の送信依頼に応じて、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化鍵ＫＰｍｅｄｉａ（１）を携帯電話機１００に対して出力する（ステップＳ４０６）。

携帯電話機１００がコンテンツデータ販売機２０００に公開暗号化鍵ＫＰｍｅｄｉａ（１）を送信し（ステップＳ４０８）、コンテンツデータ販売機２０００が、メモリカード１１０から転送された公開暗号化鍵ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ４１０）、ディスプレイ２００２を介してユーザに料金投入を案内し、料金徴収を行なう（ステップＳ４１２）。続いて、コンテンツデータ販売機２０００は、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、コンテンツデータ販売機２０００内の暗号化処理部３１６が、受信した公開暗号化鍵ＫＰｍｅｄｉａ（１）により、このセッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ４１４）。

続いて、コンテンツデータ販売機２０００は、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与え、コネクタ２０１０から出力する（ステップＳ４１６）。携帯電話機１００は、この暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を受信すると、メモリカード１１０に転送する（ステップＳ４１８）。

メモリカード１１０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を、復号処理部１４０４が、秘密復号鍵Ｋｍｅｄｉａ（１）により復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ４２０）。

続いて、配信モードにおいては、切換えスイッチ１４０８は、接点Ｐａが閉じる状態が選択されているので、暗号化処理部１４０６は、接点Ｐａを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）を、セッションキーＫｓにより暗号化し（ステップＳ４２２）、データ［ＫＰｃａｒｄ（１）］Ｋｓを生成する（ステップＳ４２４）。

携帯電話機１００は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）］Ｋｓをコンテンツデータ販売機２０００に対して送信する（ステップＳ４２６）。

コンテンツデータ販売機２０００では、コネクタ２０１０を介してデータ［ＫＰｃａｒｄ（１）］Ｋｓが受信され（ステップＳ４２８）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、公開暗号鍵ＫＰｃａｒｄ（１）を復号抽出する（ステップＳ４３０）。

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ４３２）。

さらに、コンテンツデータ販売機２０００は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、コネクタ２０１０を介して、携帯電話機１００に送信する（ステップＳ４３４）。

携帯電話機１００が暗号化コンテンツデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ４３６）、メモリカード１１０においては、受信した暗号コンテンツデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ４３８）。

一方、コンテンツデータ販売機２０００は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ４４０）、暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃとライセンス情報データＬｉｃｅｎｓ

eとを、復号処理部３１８より与えられた公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ４４２）。

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらにセッションキーＫｓにより暗号化したデータをデータバスＢＳ１に与え、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓがメモリカード１１０に対して送信される（ステップＳ４４６）。

携帯電話機１００がデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓを受信すると（ステップＳ４４８）、メモリカード１１０においては、復号処理部１４１０がセッションキーＫｓにより復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に格納する（ステップＳ４５２）。

さらに、メモリカード１１０においては、コントローラ１４２０により制御されて、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅを、レジスタ１５００に格納する（ステップＳ４５８）。

以上のような動作により、メモリカード自身が、セッションキーＫｓを送る側（コンテンツデータ販売機２０００）に、公開暗号化鍵ＫＰｍｅｄｉａ（１）を送信した上で、配信を受けることができ、メモリカード１１０に格納された暗号化コンテンツデータを用いて音楽を再生可能な状態となる。

さらに、メモリカード１１０からコンテンツデータ販売機２０００へは、携帯電話機１００を介して配信受理が通知され（ステップＳ４６０）、コンテンツデータ販売機２０００で配信受理を受信すると（ステップＳ４６２）、管理サーバに販売記録が送信され（ステップＳ４６４）、処理が終了する（ステップＳ４６６）。

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等の配信を受けることができる。

［実施の形態３の変形例］

実施の形態３のデータ配信システムにおいては、メモリカード１１０は、携帯

電話機１００を介して、コンテンツデータ販売機２０００から暗号化コンテンツデータの配信を受ける構成であった。

しかしながら、図２１に示したコンテンツデータ販売機２０００の構成において、コネクタ２０１０の代わりに、メモリカード１１０との間のインタフェースのためのメモリスロットを設ける構成とすれば、携帯電話機１００を介することなく、メモリカード１１０とコンテンツデータ販売機２０００とが直接データの授受を行なうことが可能である。

図２４は、このような実施の形態３の変形例のコンテンツデータ販売機２００１の構成を示す概念図である。図２０に示した実施の形態３のコンテンツデータ販売機２０００の構成と異なる点は、外部コネクタ２０１０の代わりに、メモリカードを挿入できるカードスロット２０３０が設けられ、このカードスロット２０３０がインタフェース部２０１２を介して、データバスＢＳ１とデータの授受をする構成となっている点である。

図２５および図２６は、実施の形態３の変形例のデータ配信システムにおける配信モードを説明するための第１および第２のフローチャートである。

図２２および図２３に示した実施の形態３の配信モードとは、携帯電話機１００を介さずに、メモリカード１１０とコンテンツデータ販売機２００１がデータの授受をする点を除いては、同様の処理であるので、同一処理には同一符号を付して、その説明は繰り返さない。

以上のような構成および動作により、一層簡易に、ユーザは暗号化された音楽データ等の配信を受けることができる。

しかも、メモリカードが独立して、暗号化コンテンツデータの配信を受け、格納できるので、コンテンツデータの再生を行なう手段の選択の幅が広がり、よりユーザの利便性が向上するという利点もある。

［実施の形態４］

図２７は、実施の形態４のコンテンツデータ販売機３０００の構成を説明するための概略ブロック図である。図２１に示したコンテンツデータ販売機２０００の構成と異なる点は、対象となるメモリカードが実施の形態２のメモリカード１２０であり、かつ使用される端末が携帯電話機１０１である点、およびこれに対

応して、データ処理部２１００における暗号化処理部３２２は、Ｋｓ発生部３１４からのセッションキーＫｓに基づいてではなく、携帯電話機に装着されたメモリカードからセッションキーＫｓにより暗号化されて送信され、復号処理部３１８により復号抽出されたセッションキー、たとえば、セッションキーＫｓ１に基づいて、暗号化処理部３２０の出力をさらに暗号化して、データバスＢＳ１を介してインタフェース部２０１２およびコネクタ２０１０に与える点である。

コンテンツデータ販売機３００.0のその他の点は、図２１に示した実施の形態3のコンテンツデータ販売機２０００の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

また、携帯電話機１０１およびメモリカード１１０の構成も実施の形態２で説明したものと同様であるので、その説明も繰り返さない。

図２８および図２９は、図２７で説明したデータ配信システムにおける配信モードを説明するための第１および第２のフローチャートである。

図２８および図２９においては、ユーザ１が、メモリカード１２０を用いることで、コンテンツデータ販売機３０００から音楽データの配信を受ける場合の動作を説明している。

まず、ユーザが、コンテンツデータ販売機３０００のキーボード２００４のキーボタンの操作等によって、配信リクエストを指示する（ステップＳ５００）。コンテンツデータ販売機３０００は、メモリカード１１０に対して公開暗号化鍵ＫＰｍｅｄｉａ（１）の送信依頼を出力する（ステップＳ５０２）。

メモリカード１２０においては、この公開暗号化鍵ＫＰｍｅｄｉａ（１）の送信依頼に応じて、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化鍵ＫＰｍｅｄｉａ（１）をコンテンツデータ販売機３０００に対して送信する（ステップＳ５０６）。さらに、メモリカード１２０においては、Ｋｓ１発生部１４３２によりセッションキーＫｓ１が生成される（ステップＳ５１５）。

携帯電話機１０１がコンテンツデータ販売機３０００に公開暗号化鍵ＫＰｍｅｄｉａ（１）を送信し（ステップＳ５０８）、コンテンツデータ販売機３０００が、メモリカード１２０から転送された公開暗号化鍵ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ５１０）、ディスプレイ２００２を介してユーザに料金投

入を案内し、料金徴収を行なう（ステップＳ５１２）。続いて、コンテンツデータ販売機３０００は、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、コンテンツデータ販売機３０００内の暗号化処理部３１６が、受信した公開暗号化鍵ＫＰｍｅｄｉａ（１）により、このセッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ５１４）。

続いて、コンテンツデータ販売機３０００は、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与え、コネクタ２０１０から出力する（ステップＳ４１６）。携帯電話機１０１は、この暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を受信すると、メモリカード１２０に転送する（ステップＳ５１８）。

メモリカード１２０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を、復号処理部１４０４が、秘密復号鍵Ｋｍｅｄｉａ（１）により復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ５２０）。

続いて、暗号化処理部１４０６は、ＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）およびＫｓ１発生部１４３２からのセッションキーＫｓ１を、セッションキーＫｓにより暗号化し（ステップＳ５２２）、データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを生成する（ステップＳ５２４）。

携帯電話機１０１は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓをコンテンツデータ販売機３０００に対して送信する（ステップＳ５２６）。

コンテンツデータ販売機３０００では、コネクタ２０１０を介してデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓが受信され（ステップＳ５２８）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ１を復号抽出する（ステップＳ５３０）。

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されてい

るデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ５３２）。

さらに、コンテンツデータ販売機３０００は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、コネクタ２０１０を介して、携帯電話機１０１に送信する（ステップＳ５３４）。

携帯電話機１０１が暗号化コンテンツデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ５３６）、メモリカード120においては、受信した暗号化コンテンツデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ５３８）。

一方、コンテンツデータ販売機３０００は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ５４０）、暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理部３１８より与えられた公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ５４２）。

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらにセッションキーＫｓ１により暗号化したデータをデータバスＢＳ１に与え、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１が携帯電話機１０１に対して出力される（ステップＳ５４６）。

携帯電話機１０１がデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を受信すると（ステップＳ５４８）、メモリカード１２０においては、復号処理部１４１０がセッションキーＫｓ１により復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に格納する（ステップＳ５５２）。

以下の処理は、図２２および図２３に示した実施の形態３の処理と同様であるので、その説明は繰り返さない。

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等のコンテンツデータ配信を受けることができる。

しかも、データバス上等で伝達されるデータの暗号化キーが、セッションごとに、かつ、機器ごとに変更されるので、データ授受のセキュリティが一層向上す

るという効果がある。

［実施の形態４の変形例］

実施の形態４のデータ配信システムにおいては、メモリカード１２０は、携帯電話機１０１を介して、コンテンツデータ販売機３０００から暗号化コンテンツデータの配信を受ける構成であった。

しかしながら、図２７に示したコンテンツデータ販売機３０００の構成において、実施の形態３の変形例と同様に、コネクタ２０１０の代わりに、メモリカード１２０との間のインタフェースのためにメモリスロットを設ける構成とすれば、携帯電話機１０１を介することなく、メモリカード１２０とコンテンツデータ販売機３０００とが直接データの授受を行なうことが可能である。

このような実施の形態４の変形例のコンテンツデータ販売機３００１の構成は、データ処理部２１００の構成を除いて、図２４に示した実施の形態３の変形例の構成と同様である。

すなわち、実施の形態４の変形例のコンテンツデータ販売機３００１の構成は、図２７に示した実施の形態４のコンテンツデータ販売機３０００の構成と異なり、外部コネクタ２０１０の代わりに、メモリカードを挿入できるカードスロット２０３０が設けられ、このカードスロット２０３０がインタフェース部２０１２を介して、データバスＢＳ１とデータの授受をする構成となっている。

図３０および図３１は、実施の形態４の変形例のデータ配信システムにおける配信モードを説明するための第１および第２のフローチャートである。

図２８および図２９に示した実施の形態３の配信モードとは、携帯電話機１０１を介さずに、メモリカード１２０とコンテンツデータ販売機３００１がデータの授受をする点を除いては、同様の処理であるので、同一処理には同一符号を付して、その説明は繰り返さない。

以上のような構成および動作により、一層簡易に、ユーザは暗号化された音楽データ等の配信を受けることができる。

しかも、メモリカードが独立して、暗号化コンテンツデータの配信を受け、格納できるので、音楽の再生を行なう手段の選択の幅が広がり、よりユーザの利便性が向上するという利点もある。

［実施の形態５］

実施の形態５の配信サーバ１２、携帯電話機１０５およびメモリカード１４０は、以下に説明するように、実施の形態２の配信サーバ１１、携帯電話機１０１およびメモリカード１２０の構成とは、以下の点で異なることを特徴とする。

すなわち、実施の形態５の携帯電話機１０５では、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこの携帯電話機１０５を登録する際に、この携帯電話機１０５に割当てられた公開暗号鍵ＫＰｐおよび証明データＣｒｔｆとを公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒにより暗号化された形で記録保持する手段を有している。

同様に、実施の形態５のメモリカード１４０でも、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこのメモリカード１４０を登録する際に、このメモリカードに割当てられた公開暗号鍵ＫＰｍｅｄｉａおよび証明データＣｒｔｆとを公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒにより暗号化された形で記録保持する手段を有している。

ここで、メモリカード１４０および実施の形態５の配信サーバ１２には、この公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒを記録保持する手段を有している。この公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒは、システム中でデータ出力を行なう全ての機器がセッションキーのやりとりに対して、相互にデータの授受を行なえる機器であることの証明と、セッションキーを相手方に送付する際に用いる暗号化鍵の獲得に用いるシステム共通の復号鍵である。

以下、さらに、実施の形態５の携帯電話機１０５、メモリカード１４０および配信サーバ１２の構成をより詳しく説明する。

図３２は、実施の形態５における携帯電話機１０５の構成を説明するための概略ブロック図である。

図１２に示した実施の形態２の携帯電話機１０１の構成と異なる点は、ＫＰｐ保持部１５２４の替わりに、公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒにより暗号化された、公開暗号鍵ＫＰｐおよび証明データＣｒｔｆを保持するための［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａｓｔｅｒ保持部１５２５を備える構成となっていることである。

携帯電話機１０５のその他の点は、図１２に示した実施の形態２の携帯電話機１０１の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図３３は、実施の形態５のメモリカード１４０に対応した配信サーバ１２の構成を示す概略ブロック図である。図１１に示した実施の形態２の配信サーバ１１の構成と異なる点は、データ処理部３１０は、公開復号鍵ＫＰｍａｓｔｅｒを保持するＫＰｍａｓｔｅｒ保持部３２４と、ＫＰｍａｓｔｅｒ保持部３２４から出力される公開復号鍵ＫＰｍａｓｔｅｒに基づいて、通信網から通信装置３５０を介してデータバスＢＳ１に与えられるデータを復号するための復号処理部３２６とをさらに備える構成となっている点である。暗号化処理部３１６は、復号処理部３２６での復号処理により抽出された公開暗号化鍵ＫＰｍｅｄｉａにより、Ｋｓ発生部３１４で発生されたセッションキーＫｓを暗号化し、また、配信制御部３１２は、復号処理部３２６での復号処理により抽出された証明データＣｒｔｆにより、配信を求めてきたメモリカードおよび携帯電話機が正規であるかの認証を行なう。

配信サーバ１２のその他の点は、図１２に示した実施の形態２の配信サーバ１１の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図３４は、本発明の実施の形態５のメモリカード１４０の構成を説明するための概略ブロック図であり、実施の形態２の図１３と対比される図である。

実施の形態５のメモリカード１４０の構成が、実施の形態２のメモリカード１２０の構成と異なる点は、まず、メモリカード１４０は、公開暗号鍵ＫＰｍｅｄｉａおよび証明データＣｒｔｆとを公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒにより暗号化された形で記録保持する[ＫＰｍｅｄｉａ，Ｃｒｔｆ] ＫＰｍａｓｔｅｒ保持部１４４２を備える構成となっていることである。一方で、切換えスイッチ１４３６は省略され、[ＫＰｍｅｄｉａ，Ｃｒｔｆ] ＫＰｍａｓｔｅｒ保持部１４４２の出力は直接データバスＢＳ３に与えられる。

さらに、メモリカード１４０は、公開復号鍵ＫＰｍａｓｔｅｒを記録保持するためのＫＰｍａｓｔｅｒ保持部１４５０と、ＫＰｍａｓｔｅｒ保持部１４５０か

ら出力される公開復号鍵ＫＰｍａｓｔｅｒに基づいて、データバスＢＳ３上のデータを復号するための復号処理部１４５２とを備える。

復号処理部１４５２での復号処理により抽出される公開暗号化鍵ＫＰｍｅｄｉａおよび証明データＣｒｔｆのうち、公開暗号化鍵ＫＰｍｅｄｉａは、暗号化処理部１４３０に与えられ、証明データＣｒｔｆは、データバスＢＳ５を介して、コントローラ１４２０に与えられる。

メモリカード１４０のその他の構成は、図１３に示したメモリカード１２０の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

［配信モード］

図３５および図３６は、図３４で説明したメモリカード１４０を用いた配信モードを説明するための第１および第２のフローチャートである。

図３５および図３６においても、ユーザ１が、メモリカード１４０を装着した携帯電話機１０５にて配信サーバ１２からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ１の携帯電話機１０５から、ユーザによりタッチキー１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

また、メモリカード１４０において保持される公開暗号化鍵ＫＰｍｅｄｉａは、他のメモリカードにおける公開暗号化鍵ＫＰｍｅｄｉａと区別するために公開暗号化鍵ＫＰｍｅｄｉａ（１）としている。さらに、メモリカード１４０、携帯電話機１０５における証明データをそれぞれＣｒｔｆ（１）、Ｃｒｔｆ（ｐ）とする。

メモリカード１４０においては、この配信リクエストに応じて、［ＫＰｍｅｄｉａ，Ｃｒｔｆ］ＫＰｍａｓｔｅｒ保持部１４４２から、公開暗号化鍵ＫＰｍｅｄｉａ（１）および証明データＣｒｔｆ（１）を暗号化したデータ［ＫＰｍｅｄｉａ（１），Ｃｒｔｆ（１）］ＫＰｍａｓｔｅｒを携帯電話機１０５に対して出力する（ステップＳ１０２´）。

携帯電話機１０５では、メモリカード１４０からのデータ［ＫＰｍｅｄｉａ

（1），Ｃｒｔｆ（1）］ＫＰｍａｓｔｅｒとともに、［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａｓｔｅｒ保持部１５２５からのデータ［ＫＰｐ，Ｃｒｔｆ（ｐ）］ＫＰｍａｓｔｅｒ、配信リクエストを配信サーバ１２に対して送信する（ステップＳ１０３）。

配信サーバ１２では、メモリカード１４０から転送された配信リクエストならびにデータ［ＫＰｐ，Ｃｒｔｆ（ｐ）］ＫＰｍａｓｔｅｒ、［ＫＰｍｅｄｉａ（1），Ｃｒｔｆ（1）］ＫＰｍａｓｔｅｒを受信すると（ステップＳ１０４´）、公開復号鍵ＫＰｍａｓｔｅｒにより復号処理部３２６が復号処理を行い、証明データＣｒｔｆ（1）、Ｃｒｔｆ（ｐ）、公開暗号化鍵ＫＰｐ、公開暗号化鍵ＫＰｍｅｄｉａ（1）の抽出を行なう（ステップＳ１０５）。

復号された証明データＣｒｔｆ（1）およびＣｒｔｆ（ｐ）に基づいて、配信制御部３１２は、配信サーバ１２に対して照会を行ない、メモリカードと携帯電話機の証明データＣｒｔｆ（1）およびＣｒｔｆ（ｐ）がともに正規の証明データの場合は次の処理に移行し（ステップＳ１０６´）、いずれかが正規の証明データでない場合には、処理を終了する（ステップＳ１５４）。

照会の結果、正規の証明データであることが確認されると、配信サーバ１２では、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、配信サーバ１２内の暗号化処理部３１６が、受信した公開暗号化鍵ＫＰｍｅｄｉａ（1）により、このセッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（1）を生成する（ステップＳ１０８）。

続いて、配信サーバ１２は、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（1）をデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３１６からの暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（1）を、通信網を通じて、携帯電話機１０５のメモリカード１４０に対して送信する（ステップＳ１１０）。

携帯電話機１０５が、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（1）を受信すると（ステップＳ１１２）、メモリカード１４０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、秘密復号鍵Ｋｍｅｄｉａ（1）で復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ１１４）。

さらに、メモリカード１４０においては、Ｋｓ１発生部１４３２によりセッションキーＫｓ１が生成される（ステップＳ１１５）。

続いて、配信モードにおいては、切換スイッチ１４０９は、接点ＰａまたはＰｂが順次閉じる状態が選択されるので、暗号化処理部１４０６は、接点Ｐａを介してセッションキー発生部１４３２から与えられるセッションキーＫｓ１と接点Ｐｂを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）（メモリカード１４０に対する公開暗号化鍵）とを、セッションキーＫｓにより暗号化し（ステップＳ１１６）、データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを生成する（ステップＳ１１８）。

携帯電話機１０５は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを配信サーバ１２に対して送信する（ステップＳ１２０）。

配信サーバ１２では、通信装置３５０によりデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓが受信され（ステップＳ１２２）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ１を復号抽出する（ステップＳ１２４）。

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ１２６）。

さらに、配信サーバ１２は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、通信装置３５０を介して、メモリカード１４０に送信する（ステップＳ１２８）。

携帯電話機１０５が暗号化コンテンツデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ１３０）、メモリカード１４０においては、受信した暗号化コンテンツデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ１３２）。

一方、配信サーバ１２は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ１３４）、暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理

部３１８より与えられた公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ１３６）。

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらに、メモリカード１４０からのセッションキーＫｓ１により暗号化したデータをデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ，（１）］Ｋｓ１をメモリカード１４０に対して送信する。

携帯電話機１０５がデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を受信すると（ステップＳ１４２）、メモリカード１４０においては、復号処理部１４１０が接点Ｐｆを介してＫｓ１発生部１４３２から与えられるセッションキーＫｓ１により復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に格納する（ステップＳ１４６）。

さらに、メモリカード１４０においては、コントローラ１４２０により制御されて、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅを、レジスタ１５００に格納する（ステップ１４８）。

以上のような動作により、メモリカード１４０自身が、暗号化コンテンツデータを送る側（配信サーバ１２）に、公開暗号化鍵ＫＰｍｅｄｉａ（１）およびセッションキーＫｓ１を送信した上で、配信を受けることができ、メモリカード１４０は、音楽を再生可能な状態となる。

さらに、メモリカード１４０から配信サーバ１２へは、配信受理が通知され、配信サーバ１２で配信受理を受信すると（ステップＳ１５０）、課金データベース３０２にユーザ１の課金データが格納され（ステップＳ１５２）、処理が終了する（ステップＳ１５４）。

以上のような配信モードでは、メモリカードおよび携帯電話機の認証がなされた上でコンテンツデータの配信が行われるので、システムのセキュリティおよび著作権の保護がより強化される。

［再生モード］

図３７および図３８は、携帯電話機１０５内において、メモリカード１４０に保持された暗号化コンテンツデータから、音楽信号を復号化し、音楽として外部に出力するための再生処理を説明する第１および第２のフローチャートである。

図３７および図３８を参照して、携帯電話機１０５のタッチキー１１０８等からのユーザ１の指示により、再生リクエストが携帯電話機１０５に対して出力される（ステップＳ２００）。

これに応じて携帯電話機１０５からは、メモリカード１４０に対して、データ［ＫＰｐ，Ｃｒｔｆ（ｐ）］ＫＰｍａｓｔｅｒが送信される（ステップＳ２４１）。

メモリカード１４０においては、データ［ＫＰｐ，Ｃｒｔｆ（ｐ）］ＫＰｍａｓｔｅｒを受信すると、復号処理部１４５２により復号処理が行われ、公開暗号化鍵ＫＰｐおよびデータＣｒｔｆの抽出が行われる（ステップＳ２４３）。

抽出された証明データＣｒｔｆに基づいて、コントローラ１４２０は、携帯電話機１０５が正規の機器であるかを判断し（ステップＳ２４５）、正規の機器と判断した場合は、処理は次のステップＳ２４６に移行し、正規の機器でないと判断した場合は、処理を終了する（ステップＳ２８０）。

正規の機器であると判断された場合、メモリカード１４０では、セッションキーＫｓ１を生成する（ステップＳ２４６）。メモリカード１４０は、さらに、抽出された公開暗号化鍵ＫＰｐによりセッションキーＫｓ１を暗号化し（ステップＳ２４８）、生成された暗号化セッションキー［Ｋｓ１］Ｋｐを携帯電話機１０５に対して送信する（ステップＳ２５０）。

携帯電話機１０５では、メモリカード１４０からの暗号化セッションキー［Ｋｓ１］Ｋｐを受信すると、復号処理部１５２２が、秘密復号鍵Ｋｐにより復号化してメモリカード１４０で生成したセッションキーＫｓ１を抽出する（ステップＳ２５２）。続いて、Ｋｓ発生部１５０２がセッションキーＫｓを生成し（ステップＳ２５３）、携帯電話機１０５の暗号化処理部１５０４は、携帯電話機１０５で生成したセッションキーＫｓをセッションキーＫｓ１により暗号化して、暗号化セッションキー［Ｋｓ］Ｋｓ１を生成し（ステップＳ２５４）、この暗号化セッションキー［Ｋｓ］Ｋｓ１をメモリカード１４０に対して送信する（ステッ

プＳ２５６）。

メモリカード１４０は、データバスＢＳ２を介して、携帯電話機１０５により生成され、かつ暗号化されたセッションキーＫｓを受け取り、セッションキーＫｓ１により復号し、携帯電話機１０５で生成したセッションキーＫｓを抽出する（ステップＳ２５８）。

続いて、メモリカード１４０において、コントローラ１４２０は、レジスタ１５００に保持されるライセンス情報データＬｉｃｅｎｓｅに基づいて、復号可能であるかを判断し（ステップＳ２５９）、復号可能と判断した場合は、次の処理に移行し、復号不可能と判断した場合は、処理を終了する（ステップＳ２８０）。

続いて、メモリカード１４０は、メモリ１４１２から、暗号化されているデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を読み出し、復号処理部１４１６が復号処理を行なう（ステップＳ２６０）。

秘密復号鍵Ｋｃａｒｄ（１）により、メモリ１４１２から読み出されたデータを復号可能な場合（ステップＳ２６２）、ライセンスキーＫｃが抽出される（ステップＳ２６４）。一方、復号不可能の場合、処理は終了する（ステップＳ２８０）。

メモリ１４１２から読み出されたデータを復号可能な場合は、さらに、レジスタ１５００内のライセンス情報データＬｉｃｅｎｓｅのうち、再生回数に関するデータが変更される（ステップＳ２６６）。

続いて、メモリカード１４０においては、暗号化処理部１４０６が、抽出したセッションキーＫｓにより、ライセンスキーＫｃを暗号化し（ステップＳ２６８）、暗号化されたライセンスキー［Ｋｃ］Ｋｓをデータバス ＢＳ２に与える（ステップＳ２７０）。

携帯電話機１０５の復号処理部１５０６は、セッションキーＫｓにより復号化処理を行なうことにより、ライセンスキーＫｃを取得する（ステップＳ２７２）。

続いて、メモリカード１４０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読み出し、データバスＢＳ２に与える（ステップＳ２７４）。

携帯電話機１０５の音楽再生部１５０８は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたライセンスキーＫｃにより復号処理して平文のコンテンツデータを生成し（ステップＳ２７６）、コンテンツデータから音楽信号を再生して混合部１５１０に与える（ステップＳ２７６）。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップＳ２３２）。

このような構成とすることで、メモリカード自身および携帯電話自身が、それぞれセッションキーＫｓ１またはＫｓを生成し、これにより暗号化コンテンツデータの授受を行なった上で、再生動作を行なうことが可能となる。

さらに、メモリカード１４０が携帯電話機１０５の認証を行なった上で、再生動作を行なうため、システムのセキュリティおよび著作権の保護が向上する。

［移動または複製モード］

図３９および図４０は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１および第２のフローチャートである。

まず、携帯電話機１０５と同様の構成を有する携帯電話機１０６が送信側であり、携帯電話機１０５が受信側であるものとする。また、携帯電話機１０６にも、メモリカード１４０と同様の構成を有するメモリカード１４２が装着されているものとする。

携帯電話機１０６は、まず、携帯電話機１０５に対して、移動リクエストまたは複製リクエストを出力する（ステップＳ３００）。

携帯電話機１０５がこのリクエストを受信すると（ステップＳ３０１）、メモリカード１４２は、これに応じて、メモリ１４１２内の暗号化コンテンツデータ［Ｄｃ］Ｋｃを読み出して、メモリカード１４０に対して出力し（ステップＳ３０２）、メモリカード１４０では、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２に格納する（ステップＳ３０４）。

続いて、携帯電話機１０６および１０５においては、ステップＳ３００において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップＳ３０６、ステップＳ３０６´）、「移動リクエス

ト」である場合、メモリカード１４０は、この移動リクエストに応じて、［ＫＰｍｅｄｉａ，Ｃｒｔｆ］ＫＰｍａｓｔｅｒ保持部１４４２から、公開暗号化鍵ＫＰｍｅｄｉａ（１）および証明データＣｒｔｆ（１）を暗号化したデータ［ＫＰｍｅｄｉａ（１），Ｃｒｔｆ（１）］ＫＰｍａｓｔｅｒを携帯電話機１０５に対して出力する（ステップＳ３０７）。

携帯電話機１０５では、メモリカード１４０からのデータ［ＫＰｍｅｄｉａ（１），Ｃｒｔｆ（１）］ＫＰｍａｓｔｅｒを携帯電話機１０６に対して送信する（ステップＳ３０８）。

携帯電話機１０６では、メモリカード１４０から転送されたデータ［ＫＰｍｅｄｉａ（１），Ｃｒｔｆ（１）］ＫＰｍａｓｔｅｒを受信すると（ステップＳ３０９）、メモリカード１４２内の復号処理部１４５２が復号処理を行い、証明データＣｒｔｆ（１）、公開暗号化鍵ＫＰｍｅｄｉａ（１）の抽出を行なう（ステップＳ３１０）。

復号された証明データＣｒｔｆ（１）に基づいて、コントローラ１４２０は、認証を行ない、正規メモリカードからのアクセスの場合は次の処理に移行し（ステップＳ３１１）、正規メモリカードでない場合には、携帯電話機１０６は移動不可の通知を送信するとともに、メモリカード１４２は処理を終了する（ステップＳ３７４）。携帯電話機１０５が移動不可通知を受信すると（ステップＳ３１３）、メモリカード１４０も処理を終了する（ステップＳ３７４）。

一方、ステップＳ３１１での照会の結果、正規メモリカードであることが確認されると、メモリカード１４２のＫｓ２発生回路１４３２は、セッションキーＫｓ２を生成し（ステップＳ３１４）、公開暗号化鍵ＫＰｍｅｄｉａ（１）を用いて、暗号化処理部１４３０がセッションキーＫｓ２を暗号化する（ステップＳ３１５）。

携帯電話機１０６は、暗号化セッションキー［Ｋｓ２］ＫＰｍｅｄｉａ（１）を携帯電話機１０５に対して送信する（ステップＳ３１６）。携帯電話機１０５は、暗号化セッションキー［Ｋｓ２］ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ３１８）、メモリカード１４０に伝達し、メモリカード１４０は、復号処理部１４０４が復号して、セッションキーＫｓ２を受理する（ステップＳ３２

0）。さらに、メモリカード１４０においてセッションキーＫｓ１が生成される（ステップＳ３２１）。

メモリカード１４０においては、セッションキーＫｓ２によりメモリカード１４０の公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ１を暗号化して（ステップＳ３２２）、携帯電話機１０５から携帯電話機１０６に対して暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ'１］Ｋｓ２を送信する（ステップＳ３２４）。携帯電話機１０６は、データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓ２を受信し（ステップＳ３２６）、メモリカード１４２に転送する。

メモリカード１４２においては、復号処理部１４１０が、メモリカード１４０から送信された暗号化データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓ２をセッションキーＫｓ２により復号化して、メモリカード１４０の公開暗号化鍵ＫＰｃａｒｄ（１）、セッションキーＫｓ１を復号抽出する（ステップＳ３３０）。

続いて、メモリカード１４２においては、メモリ１４１２からメモリカード１４２の公開暗号化鍵ＫＰｃａｒｄ（２）により暗号化されているライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅに対応する［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（２）読出される（ステップＳ３３２）。

続いて、メモリカード１４２の復号処理部１４１６が、秘密復号鍵Ｋｃａｒｄ（２）により、ライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅを復号処理する（ステップＳ３３４）。

メモリカード１４２のコントローラ１４２０は、このようにして復号されたライセンス情報データＬｉｃｅｎｓｅの値を、レジスタ１５００内のデータ値と置換する（ステップＳ３３６）。

さらに、メモリカード１４２の暗号化処理部１４１４は、復号処理部１４１０において抽出されたメモリカード１４０における公開暗号化鍵ＫＰｃａｒｄ（１）により、ライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅとを暗号化する（ステップＳ３３８）。

メモリカード１４２の暗号化処理部１４１４により暗号化されたデータは、切換スイッチ１４０９（接点Ｐｄが閉じている）を介して、さらに、暗号化処理部１４０６に与えられ、メモリカード１４２の暗号化処理部１４０６は、データ

[Kc, License] Kcard (1) をセッションキーKs1により暗号化してデータ [[Kc, License] Kcard (1)] Ks1を生成する（ステップS340）。

続いて、メモリカード142は、携帯電話機106に対してデータ [[Kc, License] Kcard (1)] Ks1を出力し（ステップS342）、携帯電話機106はデータ [[Kc, License] Kcard (1)] Ks1を携帯電話機105に対して送信する（ステップS344）。

携帯電話機105が受信したデータ [[Kc, License] Kcard (1)] Ks1は（ステップS346）、メモリカード140に対して伝達され、メモリカード140の復号処理部1410は、暗号化されたデータ [[Kc, License] Kcard (1)] Ks1を復号して、データ [Kc, License] Kcard (1) を受理する（ステップS348）。

メモリカード140においては、復号処理部1410により、セッションキーKs1に基づいて復号化処理されたデータ [Kc, License] Kcard (1) をメモリ1412に格納する（ステップS350）。さらに、メモリカード140においては、復号処理部1416が、秘密復号鍵Kcar-d (1) に基づいて、データ [Kc, License] Kcard (1) を復号し、復号されたライセンス情報データLicenseをレジスタ1500に格納する（ステップS352）。

以後の移動モードにおける処理ならびに複製モードにおけるメモリカード140および142の処理は、図18および図19で説明した実施の形態2のメモリカード120、122等の処理と同様であるので、その説明は繰り返さない。

このような構成とすることで、移動元および移動先のメモリカード自身が、セッションキーをそれぞれ生成した上で、移動動作を行なうこと、および複製動作を行なうことが可能となる。

したがって、データバス上等で伝達されるデータの暗号化キーが、セッションごとに、かつ、機器ごとに変更されるので、データ授受のセキュリティが一層向上するという効果がある。

しかも、以上のような構成を用いることで、たとえば、メモリカード142か

らメモリカード１４０へのデータの移動を、上述したようなセッションキー発生回路１５０２を有する携帯電話端末を介さずに、メモリカードとメモリカードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

ここで、移動モード時には、再生情報内の再生回数を制限するライセンス情報データについては、メモリ１４１２に記録されたライセンス情報データを、レジスタ１５００にて再生の都度修正された再生回数を記録したライセンス情報データに変更することでライセンス情報データを更新する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

しかも、メモリカード１４２がメモリカード１４０の認証を行った上で、移動動作を行なうため、システムのセキュリティおよび著作権の保護が向上する。

［実施の形態６］

図４１は、本発明の実施の形態６のコンテンツデータ販売機３０１０の構成を示す概略ブロック図であり、実施の形態４の図２７と対比される図である。

ただし、以下の説明では、実施の形態５で説明したメモリカード１４０との間のインタフェースのためにメモリスロット２０３０を設ける構成とし、実施の形態４の変形例と同様に、携帯電話機１０５を介することなく、メモリカード１４０とコンテンツデータ販売機３０１０とが直接データの授受を行なう構成であるものとする。

もちろん、コネクタ２０１０により、携帯電話機１０５を介して、メモリカード１４０とコンテンツデータ販売機３０１０とがデータの授受を行なう構成とすることも可能である。

したがって、コンテンツデータ販売機３０１０の構成が、実施の形態４のコンテンツデータ販売機３０００の構成と異なる点は、コネクタ２０１０の代わりに、メモリスロット２０３０が設けられていることと、データ処理部２１００は、公開復号鍵ＫＰｍａｓｔｅｒを保持するＫＰｍａｓｔｅｒ保持部３２４と、ＫＰｍａｓｔｅｒ保持部３２４から出力される公開復号鍵ＫＰｍａｓｔｅｒに基

づいて、通信網から通信装置３５０を介してデータバスＢＳ１に与えられるデータを復号するための復号処理部３２６とをさらに備える構成となっている点である。暗号化処理部３１６は、復号処理部３２６での復号処理により抽出された公開暗号化鍵ＫＰｍｅｄｉａにより、Ｋｓ発生部３１４で発生されたセッションキーＫｓを暗号化し、また、配信制御部３１２は、復号処理部３２６での復号処理により抽出された証明データＣｒｔｆにより、配信を求めてきたメモリカードが正規のメモリカードであるかの認証を行なう。

コンテンツデータ販売機３０１０のその他の点は、図２７に示した実施の形態4のコンテンツデータ販売機３０００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

［配信モード］

図４２および図４３は、図４１で説明したコンテンツデータ販売機３０１０を用いたデータ配信システムにおける配信動作を説明するための第１および第２のフローチャートである。

図４２および図４３においては、ユーザ１が、メモリカード１４０を用いることで、コンテンツデータ販売機３０１０からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

まず、ユーザが、コンテンツデータ販売機３０１０のキーボード２００４のキーボタンの操作等によって、配信リクエストを指示する（ステップＳ５００）。

コンテンツデータ販売機３０１０からは、メモリカード１４０に対して、認証のためのデータ［ＫＰｍｅｄｉａ，Ｃｒｔｆ］ＫＰｍａｓｔｅｒの送信依頼が出力される（ステップＳ５０２´）。

メモリカード１４０においては、この送信依頼に応じて、［ＫＰｍｅｄｉａ，Ｃｒｔｆ］ＫＰｍａｓｔｅｒ保持部１４４２から、公開暗号化鍵ＫＰｍｅｄｉａ（１）および証明データＣｒｔｆ（１）を暗号化したデータ［ＫＰｍｅｄｉａ（１），Ｃｒｔｆ（１）］ＫＰｍａｓｔｅｒをコンテンツデータ販売機３０１０に対して出力する（ステップＳ５０７）。

コンテンツデータ販売機３０１０では、メモリカード１４０から転送されたデータ［ＫＰｍｅｄｉａ（１），Ｃｒｔｆ（１）］ＫＰｍａｓｔｅｒを受信する

と、公開復号鍵ＫＰｍａｓｔｅｒにより復号処理部３２６が復号処理を行い、証明データＣｒｔｆ（１）、公開暗号化鍵ＫＰｐ、公開暗号化鍵ＫＰｍｅｄｉａ（１）の抽出を行なう（ステップＳ５０９）。

復号された証明データＣｒｔｆ（１）に基づいて、配信制御部３１２は、正規メモリカードからのアクセスかどうかの判断を行なう。正規のメモリカードの場合は次の処理に移行し（ステップＳ５１１）、正規メモリカードでない場合には、管理サーバ２２００中の管理データベースに異常終了記録を格納し（ステップＳ５６１）、処理を終了する（ステップＳ５６２）。

コンテンツデータ販売機３０１０は、ステップＳ５１１での照会の結果、正規メモリカードであることが確認されると、ディスプレイ２００２を介してユーザに料金投入を案内し、料金徴収を行なう（ステップＳ５１２）。

続いて、コンテンツデータ販売機３０１０は、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、コンテンツデータ販売機３０１０内の暗号化処理部３１６が、受信した公開暗号化鍵ＫＰｍｅｄｉａ（１）により、このセッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ５１４）。

続いて、コンテンツデータ販売機３０１０は、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与え、カードスロット２０３０から出力する（ステップＳ５１６）。

メモリカード１４０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を、復号処理部１４０４が、秘密復号鍵Ｋｍｅｄｉａ（１）により復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ５２０）。さらに、メモリカード１４０では、セッションキーＫｓ１が生成される（ステップＳ５２１）。

続いて、配信モードにおいては、切換スイッチ１４０８は、接点Ｐａが閉じる状態が選択されているので、暗号化処理部１４０６は、接点Ｐａを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）を、セッションキーＫｓにより暗号化し（ステップＳ５２２）、データ［ＫＰｃ

ａｒｄ（１）］Ｋｓを生成する（ステップＳ５２４）。

コンテンツデータ販売機３０１０では、カードスロット２０３０を介してデータ［ＫＰｃａｒｄ（１）］Ｋｓが受信され（ステップＳ５２８）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、公開暗号化鍵ＫＰｃａｒｄ（１）を復号抽出する（ステップＳ５３０）。

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ５３２）。

さらに、コンテンツデータ販売機３０１０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、カードスロット２０３０を介して、メモリカード１４０に送信する（ステップＳ５３４）。

メモリカード１４０においては、受信した暗号化コンテンツデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ５３８）。

一方、コンテンツデータ販売機３０１０は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ５４０）、暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理部３１８より与えられた公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ５４２）。

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらにセッションキーＫｓにより暗号化したデータをデータバスＢＳ１に与え、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１がメモリカード１４０に対して送信される（ステップＳ５４６）。

メモリカード１４０においては、復号処理部１４１０がセッションキーＫｓ１により復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に格納する（ステップＳ５５２）。

さらに、メモリカード１４０においては、コントローラ１４２０により制御されて、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉ

ｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅを、レジスタ１５００に格納する（ステップＳ５５４）。

以上のような動作により、メモリカード１４０は、コンテンツデータから音楽を再生可能な状態となる。

さらに、メモリカード１４０からコンテンツデータ販売機３０１０へは、配信受理が通知され（ステップＳ５５８）、コンテンツデータ販売機３０１０で配信受理を受信すると、管理サーバ２２００中の管理データベースに販売記録が送信され（ステップＳ５６０）、処理が終了する（ステップＳ５６２）。

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等のコンテンツデータの配信を受けることができる。しかも、メモリカードの認証がなされた上でコンテンツデータの配信が行われるので、システムのセキュリティおよび著作権の保護がより強化される。

［実施の形態７］

図４４は、実施の形態７における携帯電話機１０７の構成を説明するための概略ブロック図である。

図３２に示した実施の形態５の携帯電話機１０５の構成と異なる点は、携帯電話機という再生装置に共通な復号鍵Ｋｃｏｍを保持するＫｃｏｍ保持部１５３０と、復号処理部１５０６の出力を受けて、復号鍵Ｋｃｏｍについて復号し、音楽再生部１５０８にライセンスキーＫｃを与える復号処理部１５３２とを備える構成となっていることである。

携帯電話機１０７のその他の点は、図３２に示した実施の形態５の携帯電話機１０５の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。メモリカード１４０の構成も同様である。

すなわち、実施の形態７では、実施の形態５において、音楽再生部１５０８に最終的にライセンスキーＫｃと与えられる以前において、システムを構成する機器間で授受されていたライセンスキーＫｃを、実施の形態７では、さらに暗号化した［Ｋｃ］Ｋｃｏｍという状態でやり取りする以外は、実施の形態５の構成と同様である。

なお、以下の説明では、復号鍵Ｋｃｏｍは共通鍵であるものとして説明する

が、本発明はこのような場合に限定されず、たとえば、暗号化は公開鍵ＫＰｃｏｍで行い、復号化を公開暗号化鍵ＫＰｃｏｍとは非対称な秘密復号鍵Ｋｃｏｍで行なう構成としてもよい。

図４５は、実施の形態７の携帯電話機１０７に対応した配信サーバ１３の構成を示す概略ブロック図である。図３３に示した実施の形態５の配信サーバ１２の構成と異なる点は、データ処理部３１０は、復号鍵Ｋｃｏｍを保持するＫｃｏｍ保持部３３０と、配信制御部３１２を介して配信情報データベース３０４から与えられるライセンスキーＫｃを復号鍵Ｋｃｏｍにより暗号化処理して、暗号化ライセンスキー［Ｋｃ］Ｋｃｏｍとして暗号化処理部３２０に与える暗号化処理部３３２をさらに備える構成となっている点である。

配信サーバ１３のその他の点は、図３３に示した実施の形態５の配信サーバ１２の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

［配信モード］

図４６および図４７は、図４４および４５で説明した配信サーバ１３と携帯電話機１０７を用いた配信モードを説明するための第１および第２のフローチャートである。

図４６および図４７においても、ユーザ１が、メモリカード１４０を用いることで、配信サーバ１３からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

ただし、図４６および図４７の処理は、ステップＳ１３４において、配信サーバ１３が、ライセンスキーＫｃを配信情報データベース３０４より取得した後、暗号化処理部３３２がキーＫｃを暗号化して（ステップＳ１３５）、以後は、暗号化ライセンスキー［Ｋｃ］Ｋｃｏｍとして授受される点を除いては、図３５および図３６で説明した実施の形態５の配信モードと同様であるので、その説明は繰り返さない。

以上のような配信モードでは、実施の形態５に比べて、さらにシステムのセキュリティが強化される。

［再生動作］

図４８および図４９は、携帯電話機１０７内において、メモリカード１４０に保持された暗号化コンテンツデータから、音楽信号を再生し、音楽として外部に出力するための再生処理を説明する第１および第２のフローチャートである。

ただし、図４８および図４９に示した再生処理は、ステップＳ２６４でメモリカード１４０のメモリ１４１２から読み出されるキーが、暗号化ライセンスキー［Ｋｃ］Ｋｃｏｍであり、以後、暗号化ラセンスキー［Ｋｃ］Ｋｃｏｍとして携帯電話機１０７に送信され、携帯電話機１０７において、ステップＳ２７３で復号処理部１５３２によりキー［Ｋｃ］Ｋｃｏｍが復号されライセンスキーＫｃが音楽再生部１５０８に与えられる点以外は、図３７および図３８に示した実施の形態５の再生処理と同様であるのでその説明は繰り返さない。

このような構成とすることで、再生モードにおけるシステムのセキュリティおよび著作権の保護が一層向上する。

［移動または複製モード］

図５０および図５１は、実施の形態７において、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１および第２のフローチャートである。

ただし、図５０および図５１の処理は、ライセンスキーＫｃが、暗号化ライセンスキー［Ｋｃ］Ｋｃｏｍとして授受される点を除いては、図３９および図４０で説明した実施の形態５の移動または複製モードの動作と同様であるので、その説明は繰り返さない。

このような構成とすることで、移動または複製モードにおけるシステムのセキュリティおよび著作権の保護が一層向上する。

［実施の形態８］

図５２は、本発明の実施の形態８のコンテンツデータ販売機３０２０の構成を示す概略ブロック図であり、実施の形態６の図４１と対比される図である。

コンテンツデータ販売機３０２０の構成が、実施の形態６のコンテンツデータ販売機３０１０の構成と異なる点は、データ処理部２１００は、復号鍵Ｋｃｏｍを保持するＫｃｏｍ保持部３３０と、配信制御部３１２を介して配信情報データベース３０４から与えられるライセンスキーＫｃを復号鍵Ｋｃｏｍにより暗号化

処理して、暗号化ライセンスキー［Ｋｃ］Ｋｃｏｍとして暗号化処理部３２０に与える暗号化処理部３３２をさらに備える構成となっている点である。

コンテンツデータ販売機３０２０のその他の点は、図４１に示した実施の形態６のコンテンツデータ販売機３０１０の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

もちろん、実施の形態８でも、コネクタ２０１０により、携帯電話機１０７を介して、メモリカード１４０とコンテンツデータ販売機３０２０とがデータの授受を行なう構成とすることも可能である。

［配信モード］

図５３および図５４は、図５２で説明したコンテンツデータ販売機３０２０を用いたデータ配信システムにおける配信モードを説明するための第１および第２のフローチャートである。

図５３および図５４においては、ユーザ１が、メモリカード１４０を用いることで、コンテンツデータ販売機３０２０からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

ただし、図５３および図５４の処理は、ステップＳ５４０において、コンテンツデータ販売機３０２０が、ライセンスキーＫｃを配信情報データベース３０４より取得した後、暗号化処理部３３２がライセンスキーＫｃを暗号化して（ステップＳ５４１）、以後は、暗号化ライセンスキー［Ｋｃ］Ｋｃｏｍとして授受される点を除いては、図４２および図４３で説明した実施の形態５の配信動作と同様であるので、その説明は繰り返さない。

以上のような配信モードでは、実施の形態６に比べて、さらにシステムのセキュリティが強化される。

ここでは暗号化コンテンツデータを配信し、メモリカード１１０、１２０、１４０内のメモリ１４１２に格納した後、ライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅの配信を受けるように説明したが、逆にライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅを配信し、メモリカード１１０、１２０、１４０内のレジスタ１５００に格納した後、暗号化コンテンツデータの配信を受けても構わない。

さらに、移動モードにおいても配信モードと同様に、暗号化コンテンツデータ、ライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅのいずれの移動が先であっても構わない。

なお、以上説明してきた各実施の形態において、配信データとしてコンテンツデータに付随する非暗号化データ、たとえば、上記音楽データの曲名、実演者（歌手、演奏家等）、作曲家、作詞家等の当該音楽データ（コンテンツデータ）に関する著作情報や配信サーバ１０、１１、コンテンツデータ販売機３０００、３００１に対してアクセスするための情報等を、付加データＤｉとして暗号化コンテンツデータと併せて配信することも可能である。この付加データD-iは、配信、移動、複製においてはコンテンツデータとともに処理され、再生時には分離されてコンテンツデータとは個別にアクセス可能となるように、暗号化コンテンツデータと同じメモリ１４１２に格納される。

［実施の形態９］

図５５は、以上説明してきたメモリカード１１０，１２０，１４０等の端子１２０２部分の構成を説明する概略ブロック図である。

以下では、メモリカード１４０の端子１２０２部分の構成であるものとして説明する。

メモリカード１４０には、端子１２０２からシリアルにデータやコマンドが与えられる。これに対して、メモリカード１４０中のデータバスＢＳ３には、パラレルにデータやコマンドが伝達されるものとする。

図５５は、このようなメモリカード１４０へのデータ入力時のシリアル・パラレル変換と、データ出力時のパラレル・シリアル変換を行なう構成を示す概略ブロック図である。

端子１２０２中のデータピン１４６０には、データ入出力のタイミングを指定するための信号である信号ＣＳが与えられる。たとえば、信号ＣＳが活性化（“Ｌ”レベル）となった後の所定期間後に、データ入力ピン１４６２に与えられるデータが“Ｌ”レベルとなることで、データ入力のタイミングが検出される。どうように、信号ＣＳが活性化（“Ｌ”レベル）となった後の所定期間後に、データ出力ピン１４６４に出力されるデータが“Ｌ”レベルとなることで、

データ出力のタイミングが検出される。インタフェースコントローラ１４９０は、メモリカード１４０の外部からデータバスＢＳ３へのデータ入力、およびデータバスＢＳ３からメモリカード１４０外部へのデータ出力を管理する。

データ入力時は、データ入力ピン１４６２に与えられたデータは、バッファ１４６８を介して、縦列に接続されたＤ－フリップフロップ１４７０．０～１４７０．７に入力される。すなわち、８ビット分のデータが入力された時点で、Ｄ－フリップフロップ１４７０．０～１４７０．７の全てのデータが更新され、その時点で、インタフェースコントローラ１４９０により制御されて、データバッファ１４２７．０～１４２７．７からデータバスＢＳ３へデータがパラレルに出力される。

データ出力時は、データバスＢＳ３からのデータがマルチプレクサ１４７６．１～１４７６．７を介して、パラレルに与えられＤ－フリップフロップ１４７４．０～１４７４．７に格納される。その後インタフェースコントローラ１４９０により制御されて、マルチプレクサ１４７６．１～１４７６．７の接続が切換わり、Ｄ－フリップフロップ１４７４．０～１４７４．７が縦列に接続される。この状態で、Ｄ－フリップフロップ１４７４．０～１４７４．７のそれぞれに格納されたデータが、順次シリアルに、インタフェースコントローラ１４９０により制御される出力バッファ１４７０を介して、データ出力ピン１４６４から出力される。

［実施の形態９の変形例］

図５６は、データ入力の速度を向上させるために、データ入力ピンの本数を１本から２本または４本に可変とすることが可能な、メモリカード１４０の端子１２０２部分の構成の変形例を説明するための概略ブロック図である。

図５５に示した構成と異なる点は、まず、４本のデータ入力ピン１４６２．０～１４６２．３およびそれらに対応する入力バッファ１４６８．０～１４６８．３が設けられていることと、これらデータ入力ピン１４６２．０～１４６２．３に与えらたコマンドを入力バッファ１４６８．０～１４６８．３からインタフェースコントローラ１４９０に伝達するためのマルチプレクサ１４６７と、データ入力ピン１４６２．０～１４６２．３に与えらたデータまたはコマンドを、入力

バッファ１４６８．０～１４６８．３からＤ－フリップフロップ１４７０．０～１４７０．７に選択的に与えるためのマルチプレクサ１４６９．１～１４６９．７とをさらに備える構成となっていることである。

次に動作について簡単に説明する。

電源投入後には、たとえば、メモリカード１４０は、１本のデータ入力ピン１４６２．０からのみデータ入力を受けつける状態となっている。

以下では、外部からデータ入力ピン１４６２．０～１４６２．３およびマルチプレクサ１４６７を経由してインタフェースコントローラ１４９０に与えらたコマンドにより、インタフェースコントローラ１４９０がマルチプレクサ１４６９．１～１４６９．７を制御することで、４本のデータ入力ピン１４６２．０～１４６２．３からのデータをパラレルに入力するモードに動作モードが変更されたものとする。

まず、第１のタイミングで４本のデータ入力ピン１４６２．０～１４６２．３に与えられたデータは、マルチプレクサ１４６９．１～１４６９．３を経由してＤ－フリップフロップ１４７０．０～１４７０．３に与えられる。

次の第２のタイミングで、マルチプレクサ１４６９．１～１４６９．７の接続が切換わり、Ｄ－フリップフロップ１４７０．０～１４７０．３の出力がそれぞれ、Ｄ－フリップフロップ１４７０．４～１４７０．７に与えられて格納される。さらに第３のタイミングで、４本のデータ入力ピン１４６２．０～１４６２．３に与えられたデータは、マルチプレクサ１４６９．１～１４６９．３を経由してＤ－フリップフロップ１４７０．０～１４７０．３に与えられる。

以上で、８ビット分のデータのＤ－フリップフロップ１４７０．０～１４７０．７への格納が終了する。以後は、図５５の場合と同様に、データバスＢＳ３に対してパラレルに８ビット分のデータが与えられる。

データ出力の際の動作は、図５５の場合と同様である。

以上のような構成により、データ配信時、特にコンテンツデータ販売機２０００等からコンテンツデータを購入する際のメモリカード１４０へのデータ配信時間を短縮することが可能である。

また、以上説明した各実施の形態のうち、２つの携帯電話にそれぞれ装着され

た２つのメモリカード間で、たとえば、ＰＨＳのトランシーバモード等を利用することにより、コンテンツデータの移動を行なう処理を説明した実施の形態においては、このような構成に限定されず、たとえば、１つの携帯電話機に複数のメモリカードが同時装着可能な場合は、当該携帯電話機に２つのメモリカードを同時に装着することで、コンテンツデータの移動を行なう構成とすることも可能である。このようなコンテンツデータの移動の場合は、以上説明した各実施の形態において、２つの携帯電話機間での送受信のやりとりを省略すればよい。

また、以上説明した各実施の形態では、ライセンスキーＫｃは暗号化された状態で、メモリ１４１２に格納されるものとして説明したが、ライセンスキーＫｃは、復号された平文の状態でレジスタ１５００に格納されるものとしてもよい。このような構成としても、レジスタ１５００は、ＴＲＭ領域内に設けられ、外部からライセンスキーＫｃを読み出すことはできないからである。

さらに、以上説明した各実施の形態では、暗号化コンテンツデータ［Ｄｃ］Ｋｃやライセンスキーｋｃを格納するのは、携帯電話機１００等に着脱可能なメモリカードであるものとしたが、このようなメモリカードと同等の機能を有する回路を携帯電話機内に作り込む構成としてもよい。この場合は、メモリカードの種類やメモリカードごとに規定されていた鍵は、このようにして作り込まれる回路の種類やこの回路ごとに規定されるものとすればよい。

この発明を詳細に説明し示してきたが、これは例示のためのみであって、限定となってはならず、発明の精神と範囲は添付の請求の範囲によってのみ限定されることが明らかに理解されるであろう。

請求の範囲

1．コンテンツデータ供給装置から、暗号化コンテンツデータを複数のユーザの各端末に配信するためのデータ配信システムであって、

前記コンテンツデータ供給装置（１０）は、

外部との間でデータを授受するための第１のインタフェース部（３５０）と、

前記暗号化コンテンツデータの通信ごとに更新される第１の共通鍵を生成する第１のセッションキー発生部（３１４）と、

前記ユーザの端末に対応して予め定められた第１の公開暗号化鍵により前記第１の共通鍵を暗号化して前記第１のインタフェース部に与えるためのセッションキー暗号化部（３１６）と、

前記第１の共通鍵により暗号化されて返信されるデータを復号するためのセッションキー復号部（３１８）と、

前記暗号化コンテンツデータを復号するためのライセンスキーを、前記セッションキー復号部により復号されたデータを鍵データとして暗号化するための第１のライセンスデータ暗号化処理部（３２０）と、

前記第１のライセンスデータ暗号化処理部の出力を第２の共通鍵でさらに暗号化して前記第１のインタフェース部に与え配信するための第２のライセンスデータ暗号化処理部（３２２）とを備え、

各前記端末（１００）は、

外部との間でデータを授受するための第２のインタフェース部と、

前記暗号化コンテンツデータを受けて格納する配信データ解読部（１１０）とを備え、

前記配信データ解読部は、

前記第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の鍵保持部（１４０２）と、

前記第１の公開暗号化鍵によって暗号化された前記第１の共通鍵を受けて、復号処理するための第１の復号処理部（１４０４）と、

第２の公開暗号化鍵を保持するための第２の鍵保持部（１４０５）と、

前記第２の公開暗号化鍵を、前記第１の共通鍵に基づいて暗号化し、前記第２のインタフェース部に出力するための第１の暗号化処理部（１４０６）と、

前記第２のライセンスデータ暗号化処理部からの暗号化されたライセンスキーを受け、前記第２の共通鍵に基づいて復号化するための第２の復号処理部（１４１０）と、

前記ライセンスキーに基づいて復号できる前記暗号化コンテンツデータを格納するための第１の記憶部（１４１.2）と、

前記第２の公開暗号化鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する第３の鍵保持部（１４１５）と、

前記第２の復号処理部での復号結果に基づいて、前記第２の秘密復号鍵により前記ライセンスキーを復号するための第３の復号処理部（１４１６）とを備える、データ配信システム。

２．前記配信データ解読部は、前記端末に着脱可能なメモリカードであり、

前記第１の秘密復号鍵は、前記メモリカードの種類に対応して予め定められた鍵であり、

前記第２の秘密復号鍵は、前記メモリカードごとに異なる、請求項１記載のデータ配信システム。

３．前記第１の秘密復号鍵は、前記配信データ解読部の種類に対応して予め定められた鍵であり、

前記第２の秘密復号鍵は、前記配信データ解読部ごとに異なる、請求項１記載のデータ配信システム。

４．前記第２および第３の復号処理部は、前記コンテンツデータ供給装置において前記第２の公開暗号化鍵で暗号化され、さらに前記第２の共通鍵で暗号化されて、前記ライセンスキーとともに配信されるライセンス情報データを前記第２のインタフェース部を介して受け、前記第２の共通鍵および前記第２の秘密復号鍵に基づいて復号し、

前記配信データ解読部は、

復号された前記ライセンス情報データを格納する第２の記憶部（１５００）をさらに備える、請求項２記載のデータ配信システム。

5．前記第２の記憶部は、前記第３の復号処理部により復号された前記ライセンスキーをさらに格納する、請求項４記載のデータ配信システム。

6．前記第１の共通鍵と前記第２の共通鍵とは、前記暗号化コンテンツデータの通信の際に、前記第１のセッションキー発生部により生成された同一の鍵データである、請求項４記載のデータ配信システム。

7．前記配信データ解読部は、

外部から指示される再生動作モードに応じて、前記第２の記憶部に格納されたライセンス情報データにより再生可能かを判断して、前記配信データ解読部の動作を制御するための制御部をさらに備え、

前記第１の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記第３の復号処理部からの前記ライセンスキーを受けて、第３の共通鍵に基づいて暗号化して出力し、

前記第１の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力し、

各前記端末は、

前記暗号化コンテンツデータの通信ごとに更新される前記第３の共通鍵を生成する第２のセッションキー発生部（１５０２）と、

前記配信データ解読部からの前記第３の共通鍵により暗号化された前記ライセンスキーを受けて復号して抽出し、前記第１の記憶部から出力された前記暗号化コンテンツデータを前記ライセンスキーにより復号して再生するコンテンツデータ再生部（１５０６、１５０８）とをさらに備える、請求項６記載のデータ配信システム。

8．前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータおよび前記ライセンス情報データを移転するための移動動作モードに応じて、前記配信データ解読部の動作を制御するための制御部（１４２０）と、

第３の公開暗号化鍵で暗号化処理を行なうための第２の暗号化処理部（１４１４）とをさらに含み、

前記第２の復号処理部は、前記制御部に制御されて、前記移動動作モードが指

定されるのに応じて、前記第３の共通鍵に基づいて暗号化されて前記他の端末の側から送信される前記第３の公開暗号化鍵を復号して抽出し、

前記第２の暗号化処理部は、前記移動動作モードが指定されるのに応じて、前記ライセンスキーおよび前記ライセンス情報データを前記第３の公開暗号化鍵で暗号化し、

前記第１の暗号化処理部は、前記第２の暗号化処理部の出力を受けて、前記第３の共通鍵に基づいて暗号化して前記第２のインタフェース部に与え、

前記制御部は、前記移動動作モードが指定されるのに応じて、前記第２の記憶部に格納されている前記ライセンス情報データを消去し、

前記第１の記憶部は、前記移動動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第２のインタフェース部に与える、請求項７記載のデータ配信システム。

９．前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータを移転するための複製動作モードに応じて、前記配信データ解読部の動作を制御するための制御部をさらに含み、

前記第１の記憶部は、前記複製動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第２のインタフェース部に与える、請求項７記載のデータ配信システム。

１０．前記配信データ解読部は、

前記第２の共通鍵を生成するための第３のセッションキー発生部（１４３２）と、

前記第３のセッションキー発生部の出力を暗号化して前記第２のインタフェース部に与えることが可能な第３の暗号化処理部（１４３０）とをさらに含む、請求項４記載のデータ配信システム。

１１．前記配信データ解読部は、

外部から指示される再生動作モードに応じて、前記第２の記憶部に格納されたライセンス情報データにより再生可能かを判断して、前記配信データ解読部の動作を制御するための制御部をさらに備え、

前記第３の暗号化処理部は、第４の公開暗号化鍵により前記第３のセッションキー発生部の出力を暗号化して前記第２のインタフェース部に与え、

前記第１の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記第３の復号処理部からの前記ライセンスキーを受けて、第３の共通鍵に基づいて暗号化して出力し、

前記第１の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力し、

各前記端末は、

前記暗号化コンテンツデータの通信ごとに更新される前記第３の共通鍵を生成する第２のセッションキー発生部（１５０２）と、

前記第４の公開暗号化鍵を前記配信データ解読部に与える公開鍵保持部（１５２４）と、

前記第４の公開暗号化鍵で暗号化された前記第２の共通鍵を復号可能な公開鍵復号部（１５２２）と、

前記配信データ解読部からの前記第３の共通鍵により暗号化された前記ライセンスキーを受けて復号して抽出し、前記第１の記憶部から出力された前記暗号化コンテンツデータを前記ライセンスキーにより復号して再生するコンテンツデータ再生部（１５０６、１５０８）とをさらに備える、請求項１０記載のデータ配信システム。

１２．前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータおよび前記ライセンス情報データを移転するための移動動作モードに応じて、前記配信データ解読部の動作を制御するための制御部と、

第３の公開暗号化鍵で暗号化処理を行なうための第２の暗号化処理部とをさらに含み、

前記第２の復号処理部は、前記制御部に制御されて、前記移動動作モードが指定されるのに応じて、前記第３の共通鍵に基づいて暗号化されて前記他の端末の側から送信される前記第３の公開暗号化鍵を復号して抽出し、

前記第２の暗号化処理部は、前記移動動作モードが指定されるのに応じて、前

記ライセンスキーおよび前記ライセンス情報データを前記第３の公開暗号化鍵で暗号化し、

前記第１の暗号化処理部は、前記第２の暗号化処理部の出力を受けて、前記第３の共通鍵に基づいて暗号化して前記第２のインタフェース部に与え、

前記制御部は、前記移動動作モードが指定されるのに応じて、前記第２の記憶部に格納されている前記ライセンス情報データを消去し、

前記第１の記憶部は、前記移動動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第２のインタフェース部に与える、請求項１１記載のデータ配信システム。

１３．前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータを移転するための複製動作モードに応じて、前記配信データ解読部の動作を制御するための制御部をさらに含み、

前記第１の記憶部は、前記複製動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第２のインタフェース部に与える、請求項１１記載のデータ配信システム。

１４．前記第１のインタフェース部と前記第２のインタフェース部とは、携帯電話網により接続され、

前記コンテンツデータ供給装置は、

前記第１の公開暗号鍵に基づいて、前記ユーザの認証を行なう、請求項１記載のデータ配信システム。

１５．前記第１のインタフェース部は、

前記端末と直接接続可能なコネクタ部（２０１０）を含む、請求項１記載のデータ配信システム。

１６．前記第１のインタフェース部は、

前記メモリーカードと直接接続可能な接続部（２０３０）を含む、請求項２記載のデータ配信システム。

１７．コンテンツデータ供給装置から、暗号化コンテンツデータと前記暗号化データを復号するためのライセンスキーとのうちの少なくとも１つを複数のユーザ

の各端末に配信するためのデータ配信システムであって、

前記コンテンツデータ供給装置は、

外部との間でデータを授受するための第１のインタフェース部（３５０）と、

前記暗号化コンテンツデータの通信ごとに更新される第１の共通鍵を生成する第１のセッションキー発生部（３１４）と、

前記ユーザの端末に対応して予め定められた第１の公開暗号化鍵により前記第１の共通鍵を暗号化して前記第１のインタフェース部に与えるためのセッションキー暗号化処理部（３１６）と、

前記第１の共通鍵により暗号化されて返信される第２の共通鍵と第２の公開暗号化鍵を復号し抽出するセッションキー復号部（３１８）と、

前記暗号化コンテンツデータを復号するためのライセンスキーを、前記セッションキー復号部により復号された前記第２の公開暗号化鍵により暗号化するための第１のライセンスデータ暗号化処理部（３２０）と、

前記第１のライセンスデータ暗号化処理部の出力を前記第２の共通鍵でさらに暗号化して前記第１のインタフェース部に与え配信するための第２のライセンス暗号化処理部（３２２）とを備え、

各前記端末は、

外部との間でデータを授受するための第２のインタフェース部と、

前記暗号化コンテンツデータおよび前記ライセンスキーを受けて格納する配信データ解読部（１４０）とを備え、

前記配信データ解読部は、

前記第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の鍵保持部（１４０２）と、

前記第１の公開暗号化鍵によって暗号化された前記第１の共通鍵を受けて、復号処理するための第１の復号処理部（１４０４）と、

前記第２の公開暗号化鍵を保持するための第２の鍵保持部（１４０５）と、

前記第２の共通鍵を生成する第２のセッションキー発生部（１４３２）と、

前記第２の公開暗号化鍵と前記第２の共通鍵を、前記第１の共通鍵に基づいて暗号化し、前記第２のインタフェース部に出力するための第１の暗号化処理部

（１４０６）と、

前記第２のライセンスデータ暗号化処理部からの暗号化されたライセンスキーを受け、前記第２の共通鍵に基づいて復号するための第２の復号処理部（１４１０）と、

前記ライセンスキーにて復号可能な暗号化コンテンツデータを格納するための記憶部と、

前記第２の公開暗号化鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する第３の鍵保持部（１４１５）と、

前記第２の復号処理部の復号結果に基づいて、前記第２の秘密復号鍵により前記ライセンスキーを復号し抽出するための第３の復号処理部（１４１６）と、

前記第１の公開暗号化鍵を少なくとも含む第１の認証データを公開認証鍵により復号できるように暗号化して保持し外部に出力可能な第１の認証データ保持部（１４４２）とを備え、

前記コンテンツデータ供給装置は、

前記公開認証鍵により復号でき、かつ外部から与えられる前記第１の認証データを復号して抽出するための第１の認証復号処理部（３２６）と

前記第１の認証復号処理部により抽出された前記第１の認証データに基づいて認証処理を行ない、少なくともライセンスキーを配信するか否かを判断する配信制御部（３１２）をさらに含む、データ配信システム。

１８．前記記憶部は、

前記第２の復号処理部により復号された結果、前記第２の秘密復号鍵により復号可能な状態の前記ライセンスキーと前記暗号化コンテンツデータとを格納するための第１の記憶手段（１４１２）を含む、請求項１７記載のデータ配信システム。

１９．前記記憶部は、

前記暗号化コンテンツデータを格納するための第１の記憶手段（１４１２）と、

前記第３の復号処理部により復号された前記ライセンスキーを格納するための第２の記憶手段（１５００）とを含む、請求項１７記載のデータ配信システム。

２０．前記配信データ解読部は、前記端末に着脱可能なメモリカードであり、

前記第１の秘密復号鍵は、前記メモリカードの種類の対応して予め定められた値であり

前記第２の秘密複号鍵は、前記メモリカードごとに異なる、請求項１７記載のデータ配信システム。

２１．前記第１の秘密復号鍵は、前記配信データ解読部の種類の対応して予め定められた値であり

前記第２の秘密複号鍵は、前記配信データ解読部ごとに異なる、請求項１７記載のデータ配信システム。

２２．各前記端末は、コンテンツ再生部をさらに備え、

前記コンテンツ再生部は、

予め定められた第３の公開暗号鍵を少なくとも含む第２の認証データを前記公開認証鍵に基づいて復号できるように暗号化して保持し、外部に対して出力できる第２の認証データ保持部（１５２５）をさらに含む、請求項１７記載のデータ配信システム。

２３．前記第１の認証復号処理部は、

前記公開認証鍵により復号できるよう暗号化された前記第２の認証データをさらに復号して出力し、

前記配信制御部は、

前記第１の認証復号処理部にて抽出された前記第１の認証データおよび前記第２の認証データに基づいて認証処理を行ない、少なくともライセンスキーを配信するか否かを判断する、請求項２２に記載のデータ配信システム。

２４．前記第１のインタフェース部と前記第２のインタフェース部とは、携帯電話網により接続される、請求項１７記載のデータ配信システム。

２５．前記第１のインタフェース部は、

前記端末と直接接続可能なコネクタ部を含む、請求項１７記載のデータ配信システム。

２６．前記第１のインタフェース部は、

前記データ格納部と直接接続可能な接続部を含む、請求項２０記載のデータ配

信システム。

２７．前記配信データ解読部は、

前記接続部からのデータを受ける複数の端子（１４６２．０－１４６２．３）を含み、

外部からの指令に従って、前記接続部からデータを受ける端子数が切換え可能である、請求項２６記載のデータ配信システム。

２８．前記記憶部は、前記第２の復号処理部の出力を受けて、前記第２の秘密復号鍵により復号可能なように暗号化されている前記ライセンスキーを格納し、

前記コンテンツ再生部は、

前記第３の公開暗号鍵にて暗号化されたデータを復号する第３の秘密復号鍵を保持するための第４の鍵保持部（１５２０）と、

外部にて前記第３の公開暗号化鍵によって暗号化された第２の共通鍵を復号し抽出するための第４の復号処理部（１５２２）と、

第３の共通鍵を生成する第３のセッションキー発生部（１５０２）と、

前記第４の復号処理部にて復号し抽出した前記第２の共通鍵に基づいて、前記第３の共通鍵を暗号化し出力するための第２の暗号化処理部（１５０４）と、

前記コンテンツ再生部の外部にて前記第３の共通鍵に基づいて暗号化されたライセンスキーを復号し抽出するための第５復号処理部（１５０６）と、

前記記憶部に記録された暗号化コンテンツデータを、抽出した前記ライセンスキーにて復号し、再生するためのデータ再生部（１５０８）とをさらに備え、

前記配信データ解読部は、

前記公開認証鍵により復号できる前記コンテンツ再生部からの与えられる暗号化された前記第２の認証データを復号して前記第３の公開暗号化鍵を抽出するための第２の認証復号処理部（１４５２）と、

前記第２のセッションキー発生部にて生成した前記第２の共通鍵を前記第３の公開暗号化鍵に基づいて暗号化する第３の暗号化処理部（１４３０）と、

前記コンテンツ再生部にて前記第２の共通鍵にて暗号化された前記第３の共通鍵を受けて、前記第２の復号処理部（１４１０）にて前記第２の共通鍵に基づいて復号した前記第３の共通鍵に基づいて、前記記憶部に格納されたデータを前記

第２の秘密復号鍵にて復号した前記ライセンスキーを、前記第１の暗号化処理部にて暗号化し、前記コンテンツ再生部へ出力を指示する制御部（１４２０）とをさらに備え、

前記制御部は、前記第２の認証復号処理部により復号された前記第２の認証データに基づいて認証処理を行ない、少なくともライセンスキーを出力するか否かを判断する、請求項２２記載のデータ配信システム。

２９．前記記憶部は、前記第２の復号処理部の出力を受けて、前記第２の秘密復号鍵により復号可能なように暗号化されている前記ライセンスキーを格納し、

前記配信データ解読部は、

他の端末の配信データ解読部に対して少なくとも前記ライセンスキーを移転するために、前記配信データ解読部の外部から指示される移動処理に応じて、前記他の配信データ解読部からの前記公開認証鍵によって復号できる暗号化された第１の認証データを、前記公開認証鍵にて復号して、前記他の配信データ解読部における前記第１の公開暗号化鍵を抽出する第２の認証復号処理部（１４５２）と、

前記他の配信データ解読部の前記第１の公開暗号化鍵によって前記第２の共通鍵を暗号化するための第３の暗号化処理部（１４３０）と、

前記他の配信データ解読部の第２の公開暗号化鍵による暗号化処理を行うための第４の暗号化処理部（１４１４）とをさらに含み、

前記第２のセッションキー発生部は、前記移動処理に応じて、前記第２の共通鍵を発生し、

前記第２の復号処理部は、前記移動処理に応じて、前記他の配信データ解読部から前記第２の共通鍵によって暗号化され、入力される第４の共通鍵と前記他の配信データ解読部の第２の公開暗号化鍵とを復号して抽出し、

前記第３の復号処理部は、前記移動処理に応じて、前記第２の秘密復号鍵に基づいて、前記記憶部に格納された前記第２の公開暗号化鍵にて暗号化されたデータを復号して、ライセンスキーを抽出し、

前記第４の暗号化処理部は、前記移動処理に応じて、前記他の配信データ解読部の第２の公開暗号化鍵に基づいて、抽出された前記ライセンスキーを暗号化

し、

前記第１の暗号化処理部は、前記移動処理に応じて、前記第４の暗号化処理部の出力を前記第４の共通鍵にて暗号化し、前記他の配信データ解読部に対して出力し、

前記制御手段は、前記第２の認証復号処理部により抽出された前記他のデータ解読部から出力された第２の認証データに基づき認証処理を行ない、少なくともライセンスキーを出力するか否かを判断する、請求項２０記載のデータ配信システム。

３０．前記他の配信データ解読部は、

前記認証復号処理においては、前記配信データ解読部から少なくとも前記ライセンスキーを移転するための前記他の配信データ解読部の外部から指示される移動処理に応じて、前記第１の認証データ保持部が前記第１の認証データを出力し、

前記第１の復号処理部は、前記移動処理に応じて、前記配信データ解読部から前記第１の公開暗号化鍵によって暗号化され、入力される前記配信データ解読部にて発生された前記第２の共通鍵を復号して抽出し、

前記第２のセッションキー発生部は、前記移動受理処理に応じて、前記第４の共通鍵を発生し、

前記第１の暗号化処理部は、前記移動受理処理に応じて、第２の共通鍵に基づいて、前記第２の公開暗号化鍵と前記第４の共通鍵とを暗号化して出力し、

前記第２の復号処理部は、前記配信データ解読部において前記第２の公開暗号化鍵にて暗号化され、さらに前記第４の共通鍵にて暗号化されたライセンスキーを前記第４の共通鍵にて復号し、前記記憶部に記録する請求項２９記載のデータ配信システム。

３１．前記コンテンツデータ供給装置は、

前記コンテンツ再生部と共通な第５の共通鍵を保持する第５の鍵保持部と、

前記第５の鍵保持部に保持された前記第５の共通鍵に基づいて、前記ライセンスキーを暗号化し前記第１のライセンス暗号化処理部に対して出力する第３のライセンス暗号化部をさらに含み、

前記コンテンツ再生部は、

前記第５の共通鍵を保持する第６の鍵保持手段と、

前記第４の復号処理部と前記データ再生部との間に設けられ、前記第６の鍵保持部に保持された前記第５の共通鍵によって、前記第４の復号処理部の出力から前記ライセンスキーを復号し抽出し、前記データ再生部に対して出力する第５の復号処理部をさらに含む、請求項２６記載のデータ配信システム。

３２．前記コンテンツデータ供給装置は、

前記コンテンツ再生部にて復号可能な第４の公開暗号化鍵を保持する第５の鍵保持部と、

第４の公開暗号化鍵に基づいて前記ライセンスキーを暗号化し前記第１のライセンス暗号化処理部にて出力する第３のライセンス暗号化部をさらに含み、

前記コンテンツ再生部は、

第４の公開暗号化鍵によって暗号化されたデータを復号できる第４の秘密復号鍵を保持する第６の鍵保持手段と、

前記第４の復号処理部と前記データ再生部との間に設けられ、第４の秘密復号鍵によって前記第４の復号処理部の出力から前記ライセンスキーを復号し抽出し、前記データ再生部に対して出力する第５の復号処理部をさらに含む、請求項２６記載のデータ配信システム。

３３．前記端末は、

複数の配信データ解読部を備える、請求項２０記載のデータ配信システム。

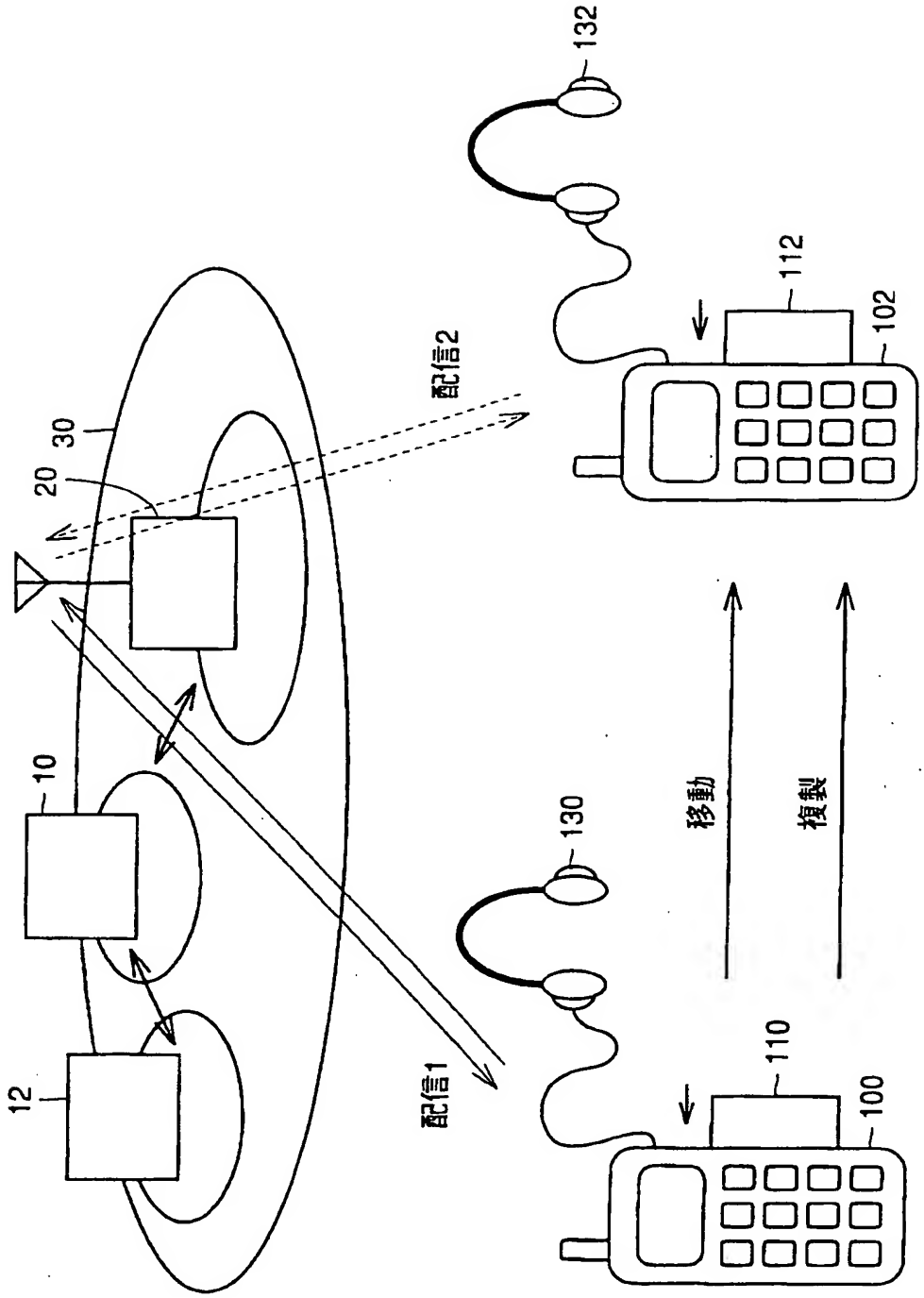


FIG.1

FIG.2

	記号	属性	特性	
メモリカード内管理の鍵	Kmedia(n)	秘密復号鍵	媒体固有	メモリカードの種類ごとに固有な情報を有する
	Kcard(n)	秘密復号鍵		メモリカード毎に異なる
	KPcard(n)	公開暗号化鍵		Kcard(n)と対を成す。 KPcard(n)により暗号化されたデータは、Kcard(n)で復号可能
メモリカード外管理の鍵	KPmedia(n)	公開暗号化鍵	媒体固有	Kmediaと対を成す。 KPmediaにより暗号化されたデータは、Kmediaで復号可能。
	Ks	共通鍵	セッション固有	通信毎（例：アクセス毎）に発生。 配信サーバ、携帯電話機にて管理
配信データ	Kc	共通鍵	ライセンスキー	暗号化コンテンツデータの復号鍵
	License-ID	再生に関する情報		例：曲目の特定情報 再生回数の制限情報
	User-ID	受信者を識別する情報		例：電話番号
	Dc	コンテンツデータ		例：音楽
	[Dc]Kc	暗号化コンテンツデータ		共通鍵Kcにより暗号化されたコンテンツデータ

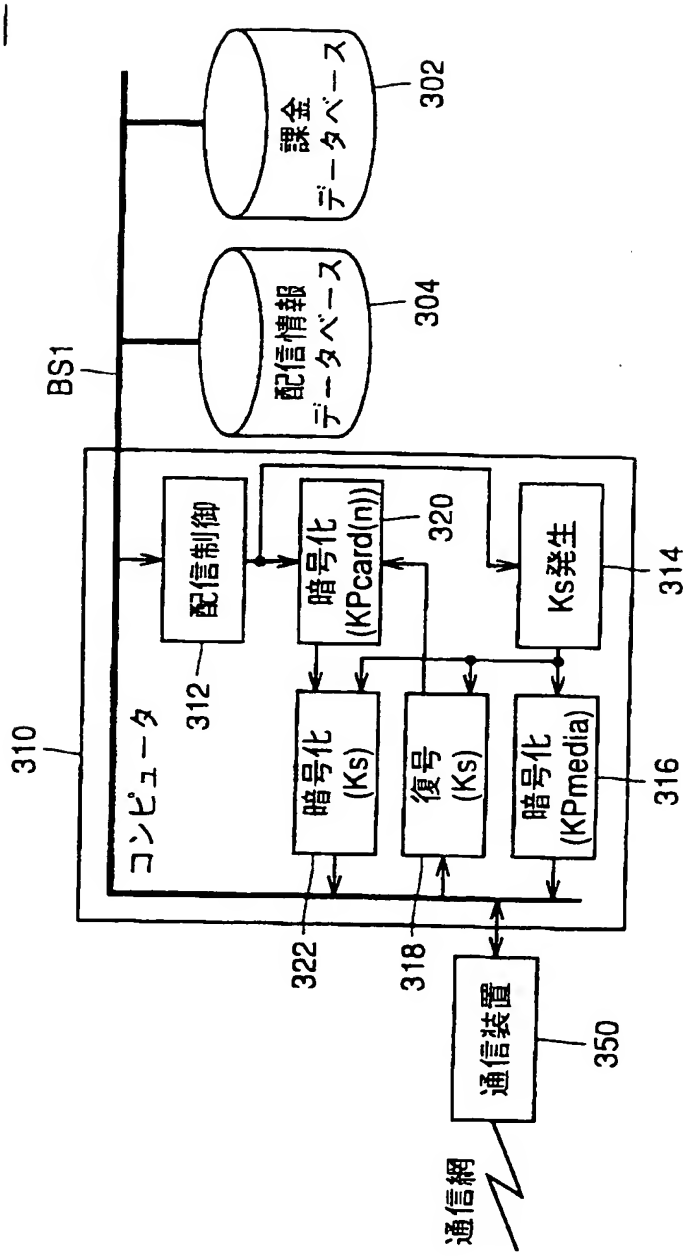

10
課金
データベース
302
配信情報
データベース
304
BS1
配信制御
312
暗号化
(KPcard(n))
320
Ks発生
314
コンピュータ
310
暗号化
(Ks)
復号
(Ks)
暗号化
(KPmedia)
316
322
318
通信装置
350
通信網

FIG.3

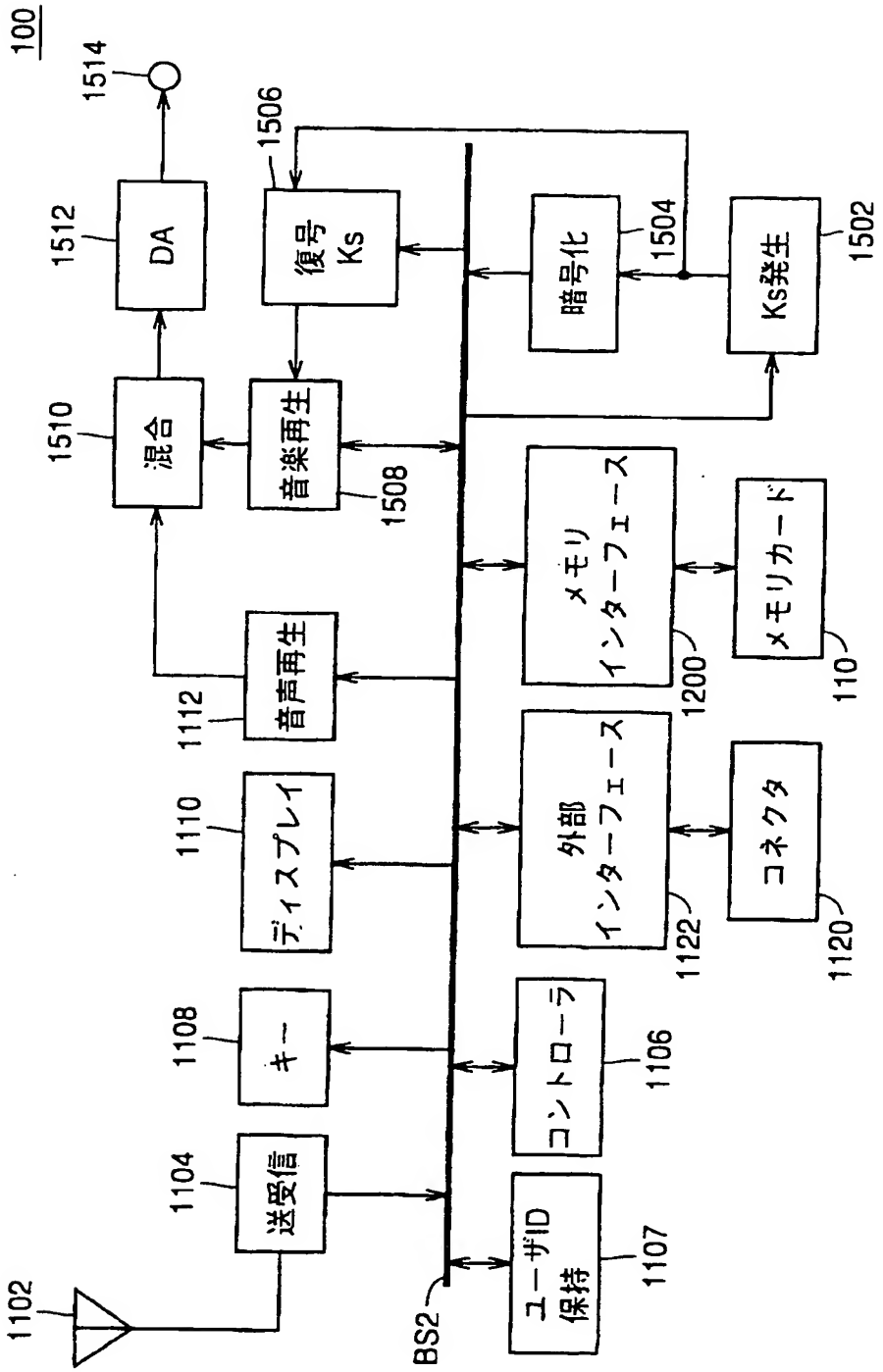

100
1514
1506
1512
DA
復号
Ks
暗号化
1504
Ks発生
1502
1510
混合
音楽再生
1508
メモリ
インターフェース
メモリカード
1200
110
1112
音声再生
1110
ディスプレイ
外部
インターフェース
コネクタ
1122
1120
1108
キー
コントローラ
1106
1104
送受信
ユーザID
保持
1107
1102
BS2

FIG.4

FIG.5

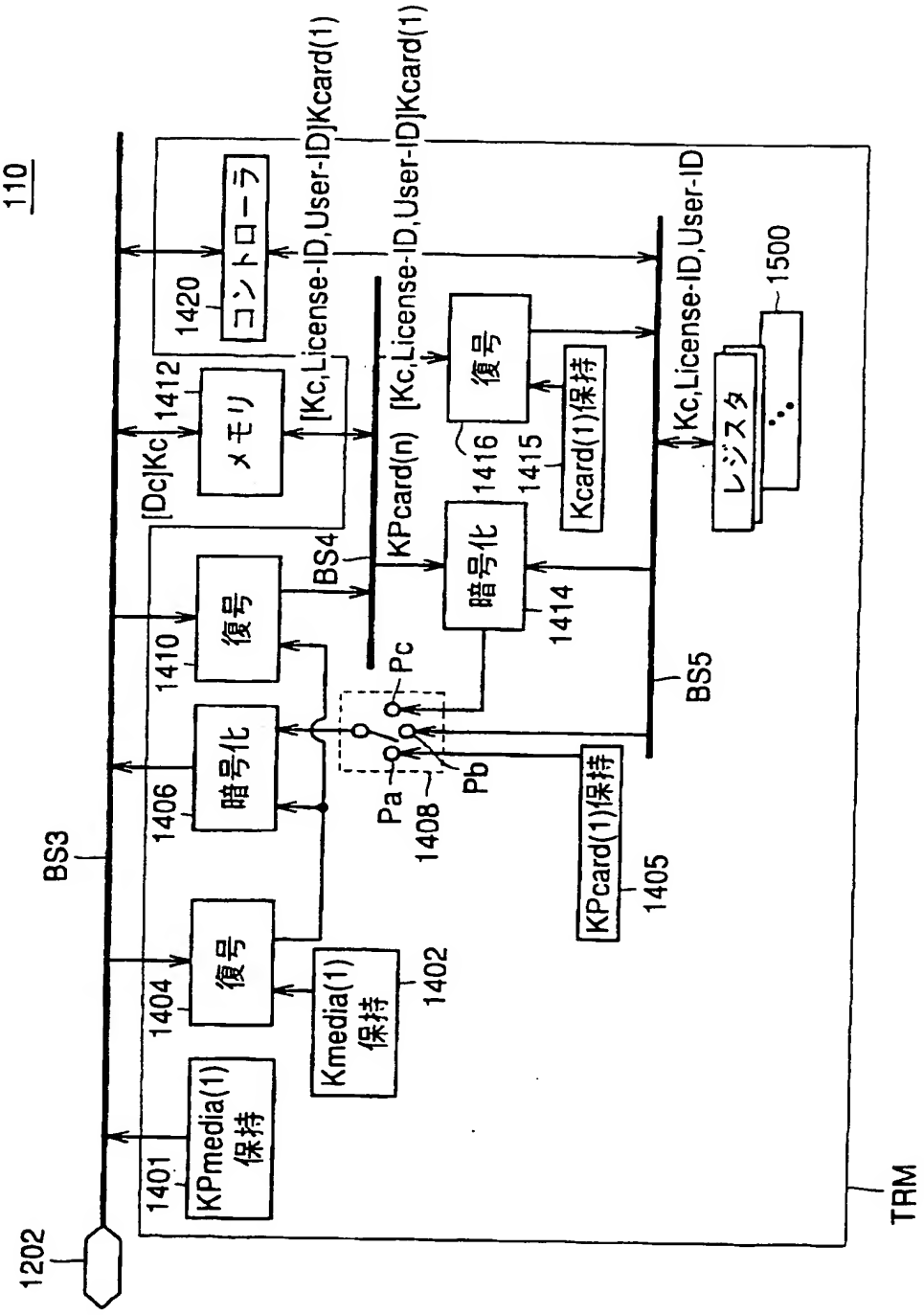

110
1202
BS3
1401
KPmedia(1)保持
1404
復号
Kmedia(1)保持
1402
1406
暗号化
1410
復号
BS4
[Dc]Kc
1412
メモリ
[Kc,License-ID,User-ID]Kcard(1)
1420
コントローラ
KPcard(n)
[Kc,License-ID,User-ID]Kcard(1)
Pa
Pb
Pc
1408
KPcard(1)保持
1405
暗号化
1414
復号
1416
Kcard(1)保持
1415
BS5
Kc,License-ID,User-ID
レジスタ
1500
TRM

FIG.6

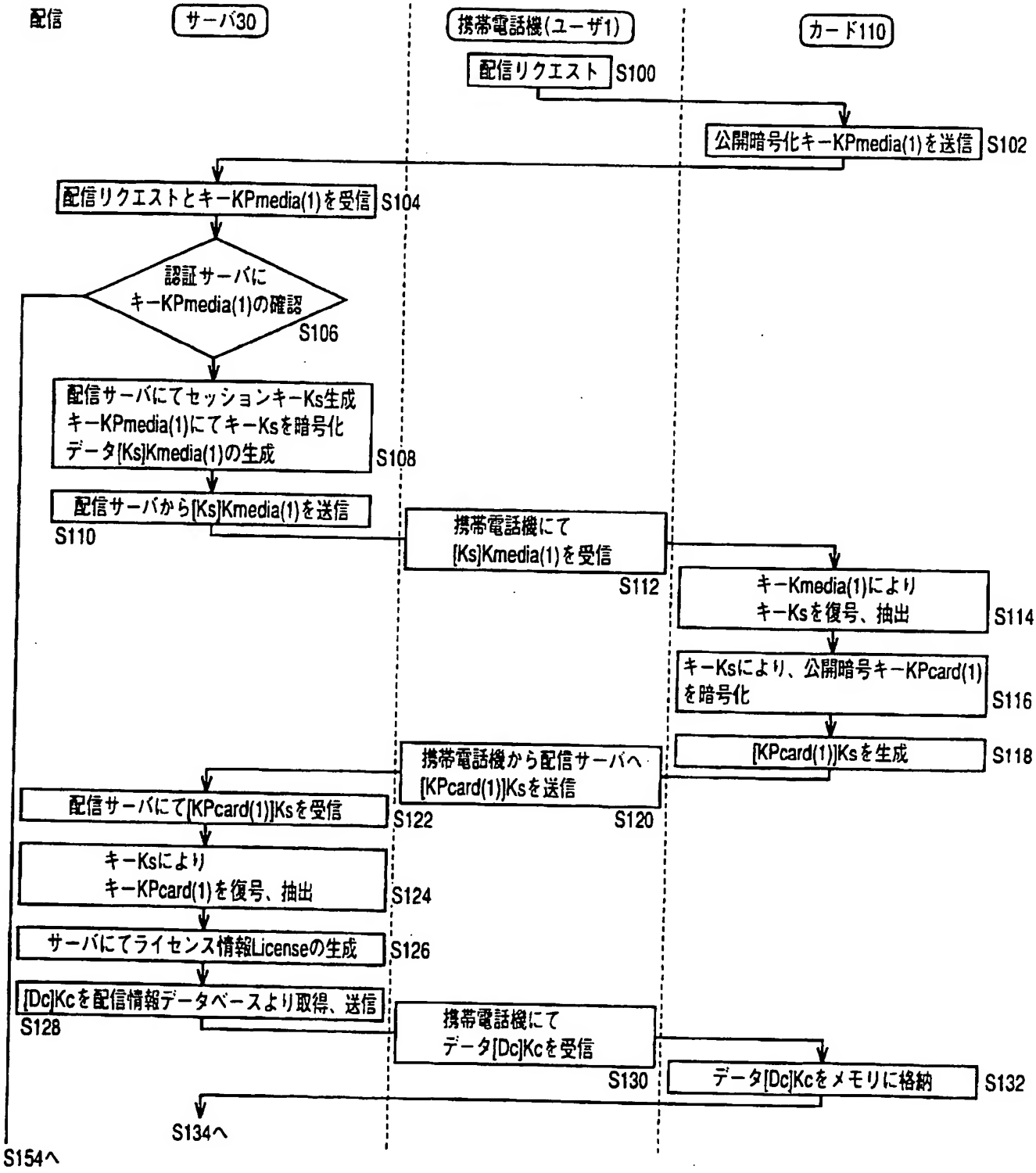

配信
サーバ30
携帯電話機(ユーザ1)
カード110
配信リクエスト S100
公開暗号化キーKPmedia(1)を送信 S102
配信リクエストとキーKPmedia(1)を受信 S104
認証サーバに
キーKPmedia(1)の確認
S106
配信サーバにてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成 S108
配信サーバから[Ks]Kmedia(1)を送信
S110
携帯電話機にて
[Ks]Kmedia(1)を受信
S112
キーKmedia(1)により
キーKsを復号、抽出 S114
キーKsにより、公開暗号キーKPcard(1)
を暗号化 S116
[KPcard(1)]Ksを生成 S118
携帯電話機から配信サーバへ
[KPcard(1)]Ksを送信
S120
配信サーバにて[KPcard(1)]Ksを受信
S122
キーKsにより
キーKPcard(1)を復号、抽出 S124
サーバにてライセンス情報Licenseの生成 S126
[Dc]Kcを配信情報データベースより取得、送信
S128
携帯電話機にて
データ[Dc]Kcを受信
S130
データ[Dc]Kcをメモリに格納 S132
S134へ
S154へ

FIG.7

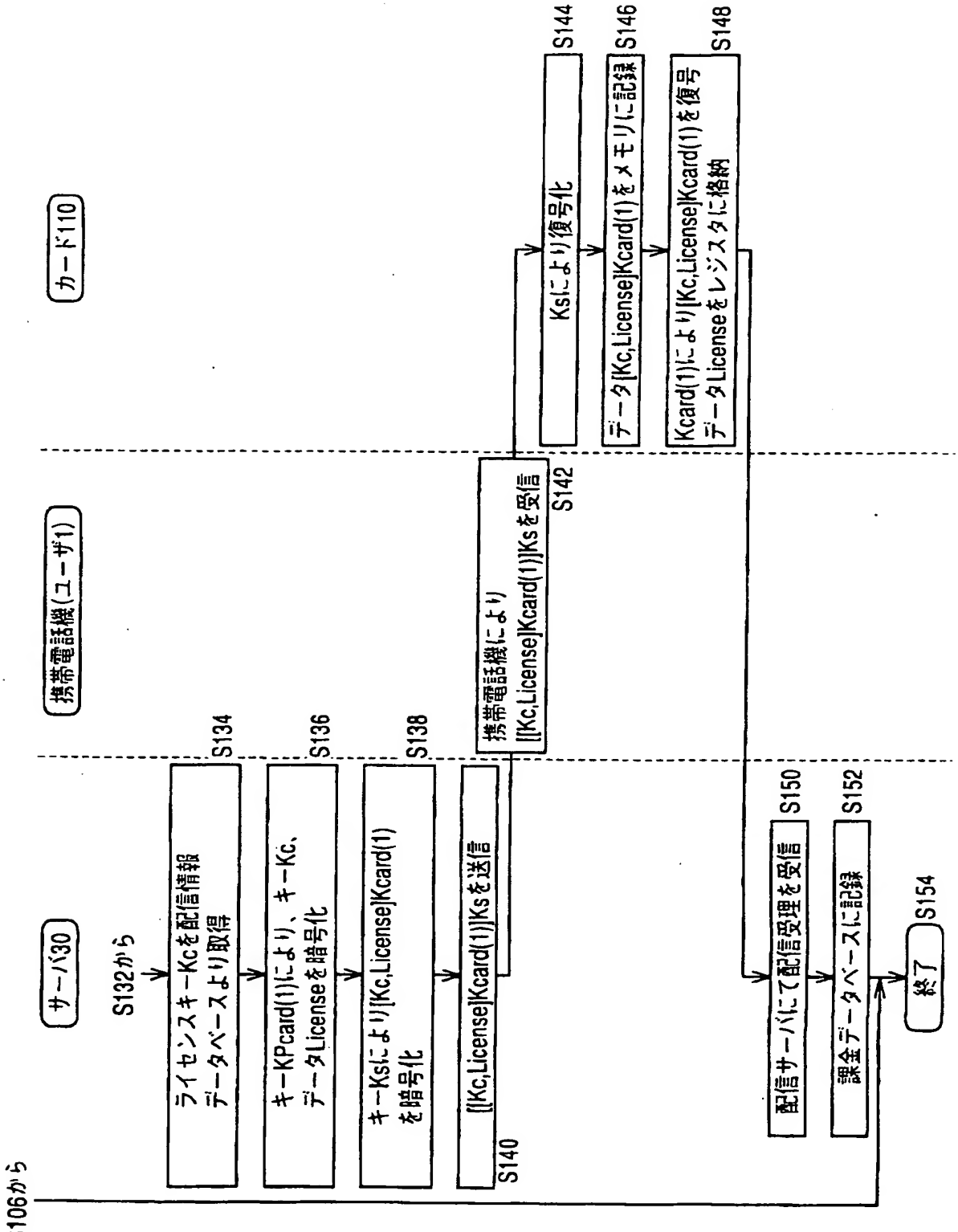

S106から
サーバ30
携帯電話機(ユーザ1)
カード110
S132から
ライセンスキーKcを配信情報データベースより取得
S134
キーKPcard(1)により、キーKc、データLicenseを暗号化
S136
キーKsにより[Kc,License]Kcard(1)を暗号化
S138
[[Kc,License]Kcard(1)]Ksを送信
S140
携帯電話機により[[Kc,License]Kcard(1)]Ksを受信
S142
Ksにより復号化
S144
データ[Kc,License]Kcard(1)をメモリに記録
S146
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S148
配信サーバにて配信受理を受信
S150
課金データベースに記録
S152
終了
S154

FIG.8

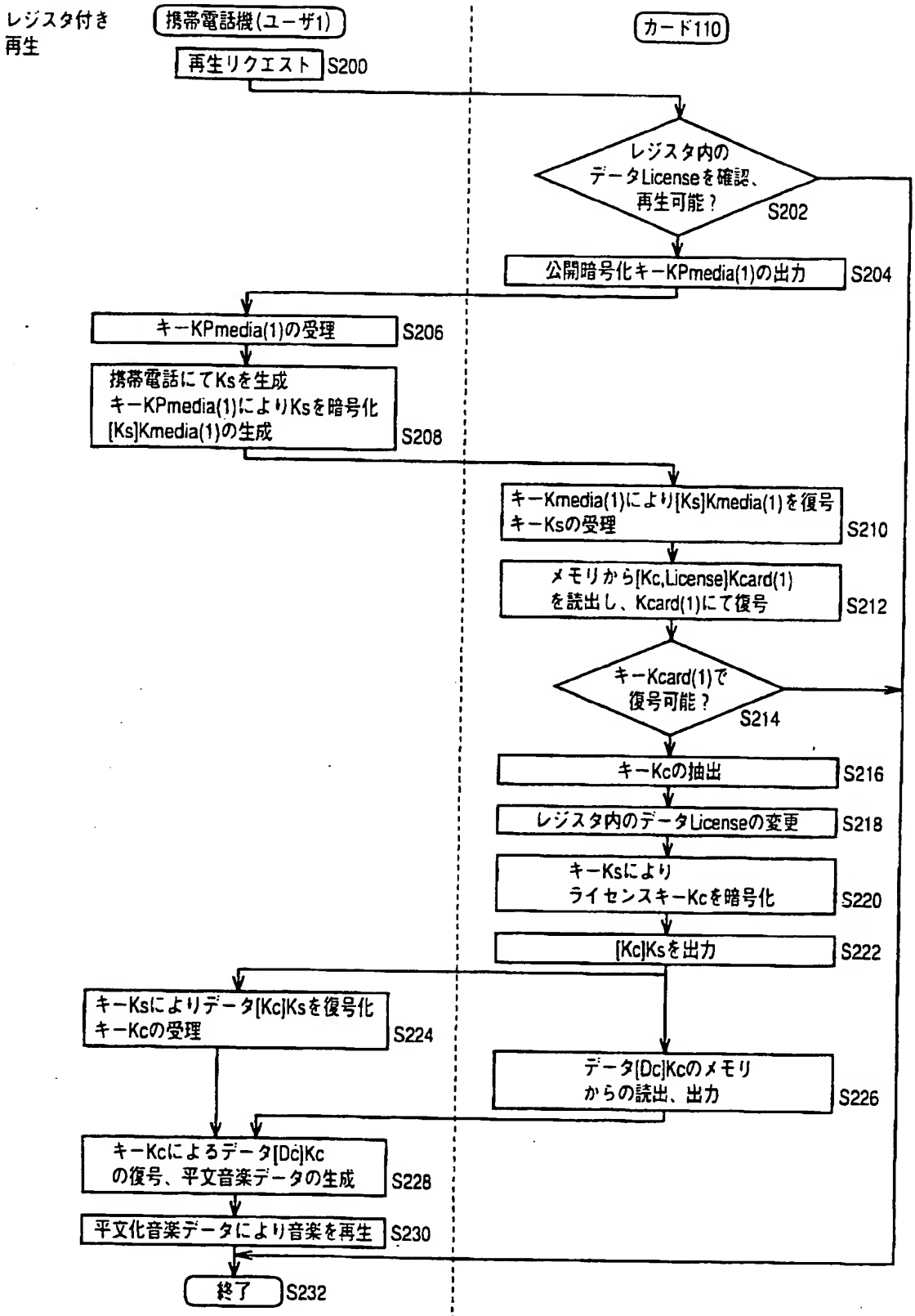

レジスタ付き再生
携帯電話機(ユーザ1)
カード110
再生リクエスト S200
レジスタ内のデータLicenseを確認、再生可能？ S202
公開暗号化キーKPmedia(1)の出力 S204
キーKPmedia(1)の受理 S206
携帯電話にてKsを生成
キーKPmedia(1)によりKsを暗号化
[Ks]Kmedia(1)の生成 S208
キーKmedia(1)により[Ks]Kmedia(1)を復号
キーKsの受理 S210
メモリから[Kc,License]Kcard(1)を読出し、Kcard(1)にて復号 S212
キーKcard(1)で復号可能？ S214
キーKcの抽出 S216
レジスタ内のデータLicenseの変更 S218
キーKsによりライセンスキーKcを暗号化 S220
[Kc]Ksを出力 S222
キーKsによりデータ[Kc]Ksを復号化
キーKcの受理 S224
データ[Dc]Kcのメモリからの読出、出力 S226
キーKcによるデータ[Dc]Kcの復号、平文音楽データの生成 S228
平文化音楽データにより音楽を再生 S230
終了 S232

FIG.9

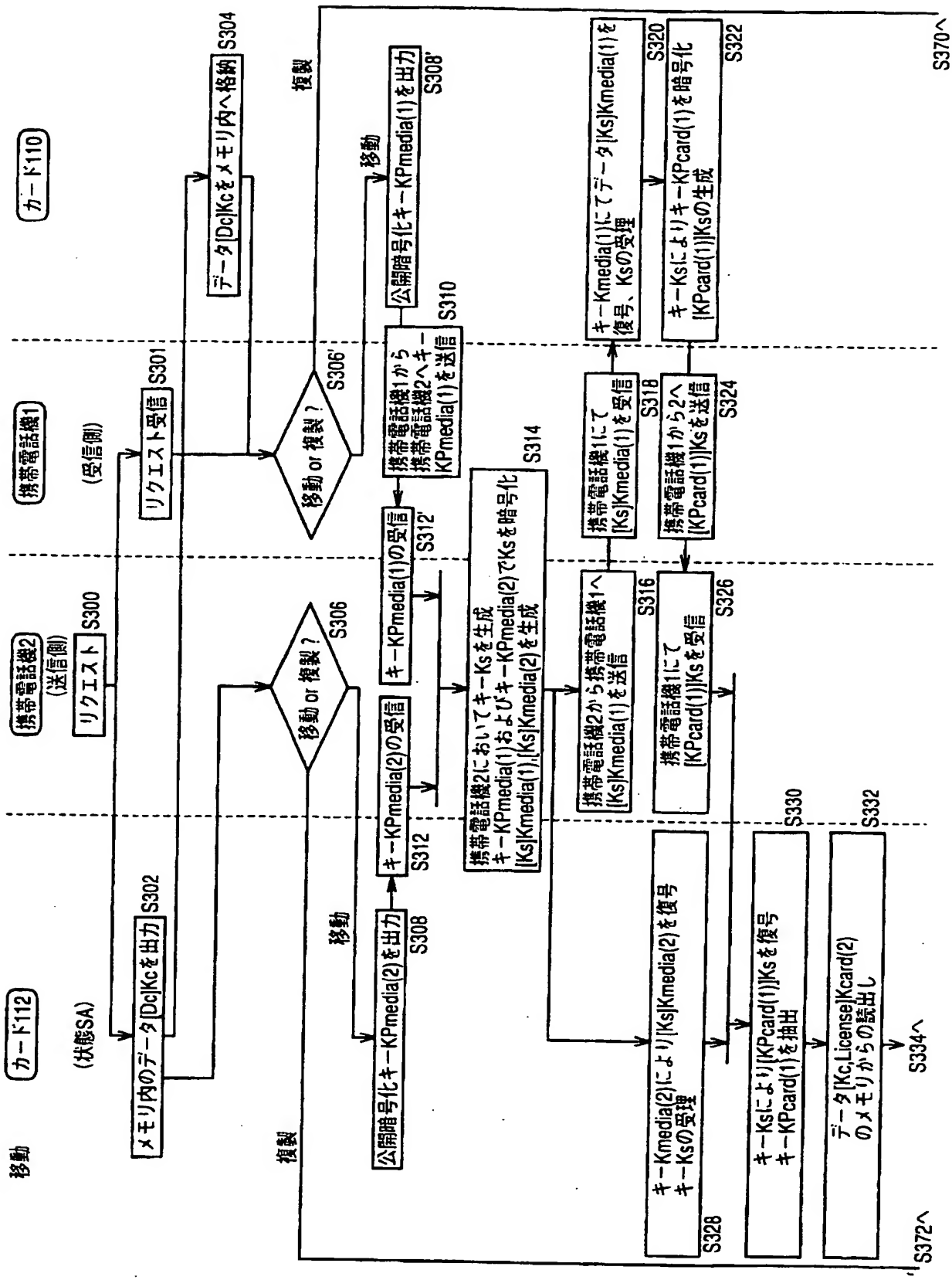
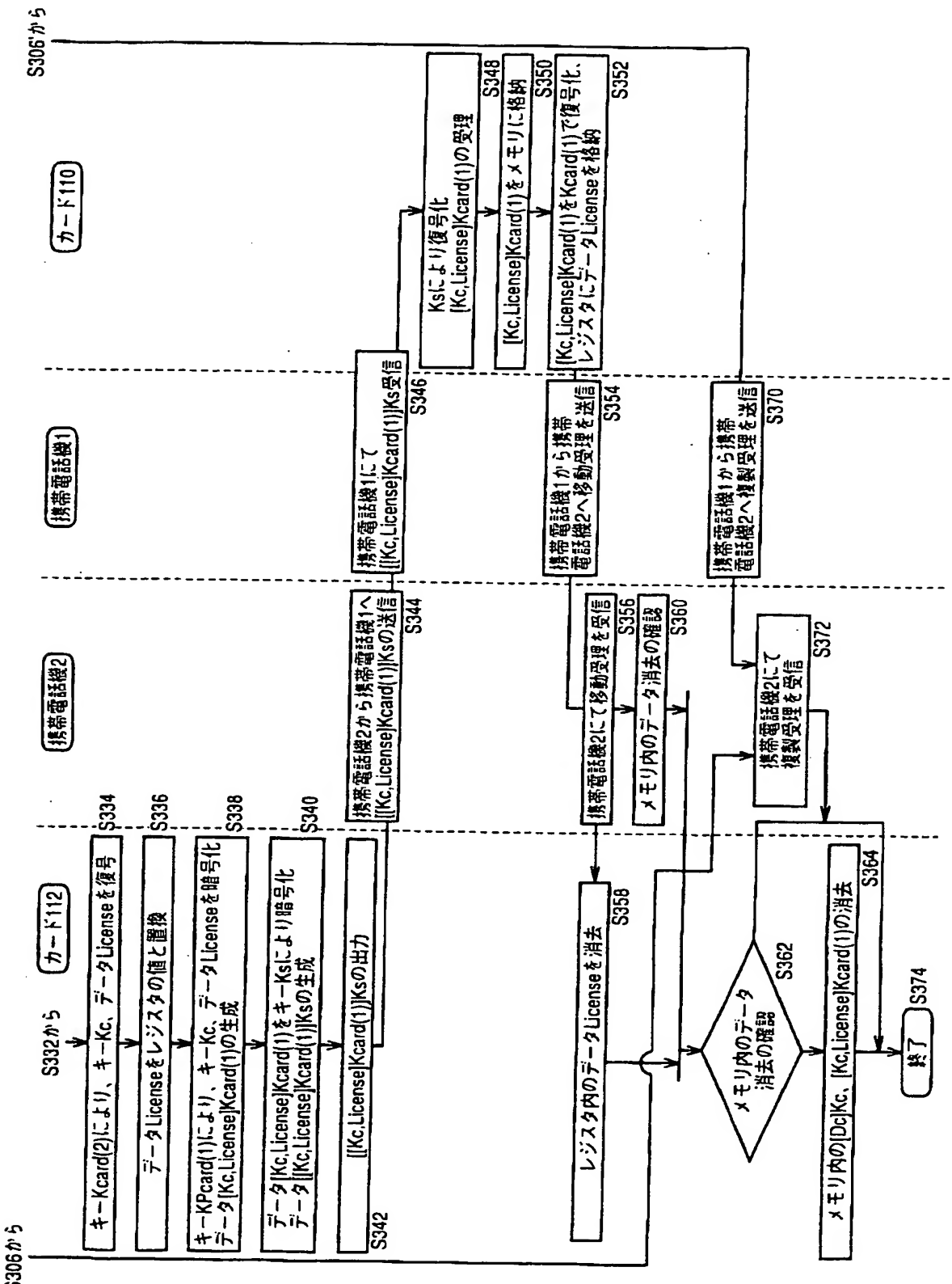

移動
カード112
携帯電話機2
(送信側)
携帯電話機1
(受信側)
カード110
(状態SA)
リクエスト S300
リクエスト受信 S301
メモリ内のデータ[Dc]Kcを出力 S302
データ[Dc]Kcをメモリ内へ格納 S304
移動 or 複製? S306
移動
複製
公開暗号化キーKPmedia(2)を出力 S308
キーKPmedia(2)の受信 S312
公開暗号化キーKPmedia(1)を出力 S308'
キーKPmedia(1)の受信 S312'
携帯電話機2から携帯電話機1へ
キーKPmedia(1)およびキーKPmedia(2)を送信 S310
携帯電話機2においてキーKsを生成
キーKPmedia(1)および[Ks]Kmedia(2)でKsを暗号化
[Ks]Kmedia(1),[Ks]Kmedia(2)を生成 S314
携帯電話機2から携帯電話機1へ
[Ks]Kmedia(1)を送信 S316
携帯電話機1にて
[Ks]Kmedia(1)を受信 S318
キーKmedia(1)にてデータ[Ks]Kmedia(1)を
復号、Ksの受理 S320
携帯電話機1から2へ
[KPcard(1)]Ksを送信 S324
キーKsにより[KPcard(1)]Ksを暗号化
[KPcard(1)]Ksの生成 S322
携帯電話機1にて
[KPcard(1)]Ksを受信 S326
キーKmedia(2)により[Ks]Kmedia(2)を復号
キーKsの受理 S328
キーKsにより[KPcard(1)]Ksを復号
キーKPcard(1)を抽出 S330
データ[Kc,License]Kcard(2)
のメモリからの読出し S332
S334へ
S370へ
S372へ

FIG.10


S306から
カード110
携帯電話機1
携帯電話機2
カード112
S332から
キーKcard(2)により、キーKc、データLicenseを復号
S334
データLicenseをレジスタの値と置換
S336
キーKPcard(1)により、キーKc、データLicenseを暗号化
データ[Kc,License]Kcard(1)の生成
S338
データ[Kc,License]Kcard(1)をキーKsにより暗号化
データ[[Kc,License]Kcard(1)]Ksの生成
S340
[[Kc,License]Kcard(1)]Ksの出力
S342
携帯電話機2から携帯電話機1へ
[[Kc,License]Kcard(1)]Ksの送信
S344
携帯電話機1にて
[[Kc,License]Kcard(1)]Ks受信
S346
Ksにより復号化
[Kc,License]Kcard(1)の受理
S348
[Kc,License]Kcard(1)をメモリに格納
S350
[Kc,License]Kcard(1)をKcard(1)で復号化、
レジスタにデータLicenseを格納
S352
携帯電話機1から携帯
電話機2へ移動受理を送信
S354
携帯電話機2にて移動受理を受信
S356
メモリ内のデータ消去の確認
S360
携帯電話機1から携帯
電話機2へ複製受理を送信
S370
携帯電話機2にて
複製受理を受信
S372
レジスタ内のデータLicenseを消去
S358
メモリ内のデータ
消去の確認
S362
メモリ内の[Dc]Kc、[Kc,License]Kcard(1)の消去
S364
終了
S374

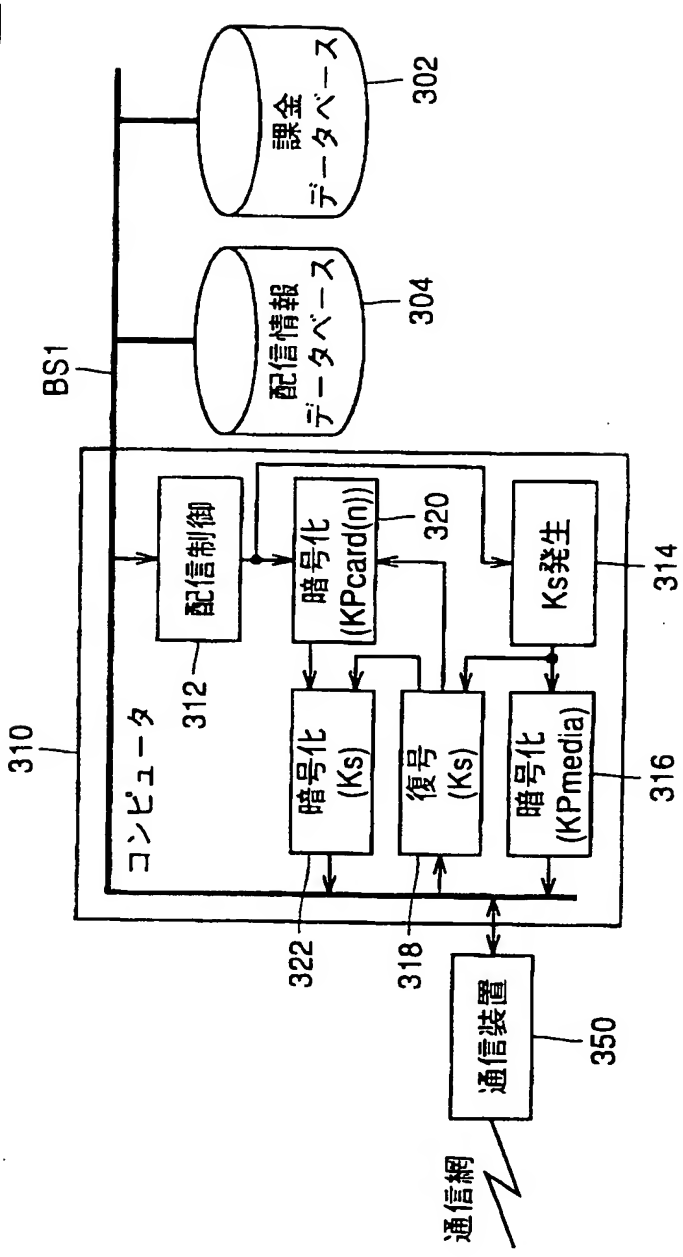

11
課金データベース
302
配信情報データベース
304
BS1
配信制御
312
暗号化(KPcard(n))
320
Ks発生
314
コンピュータ
310
暗号化(Ks)
復号(Ks)
暗号化(KPmedia)
316
322
318
通信装置
350
通信網

FIG.11

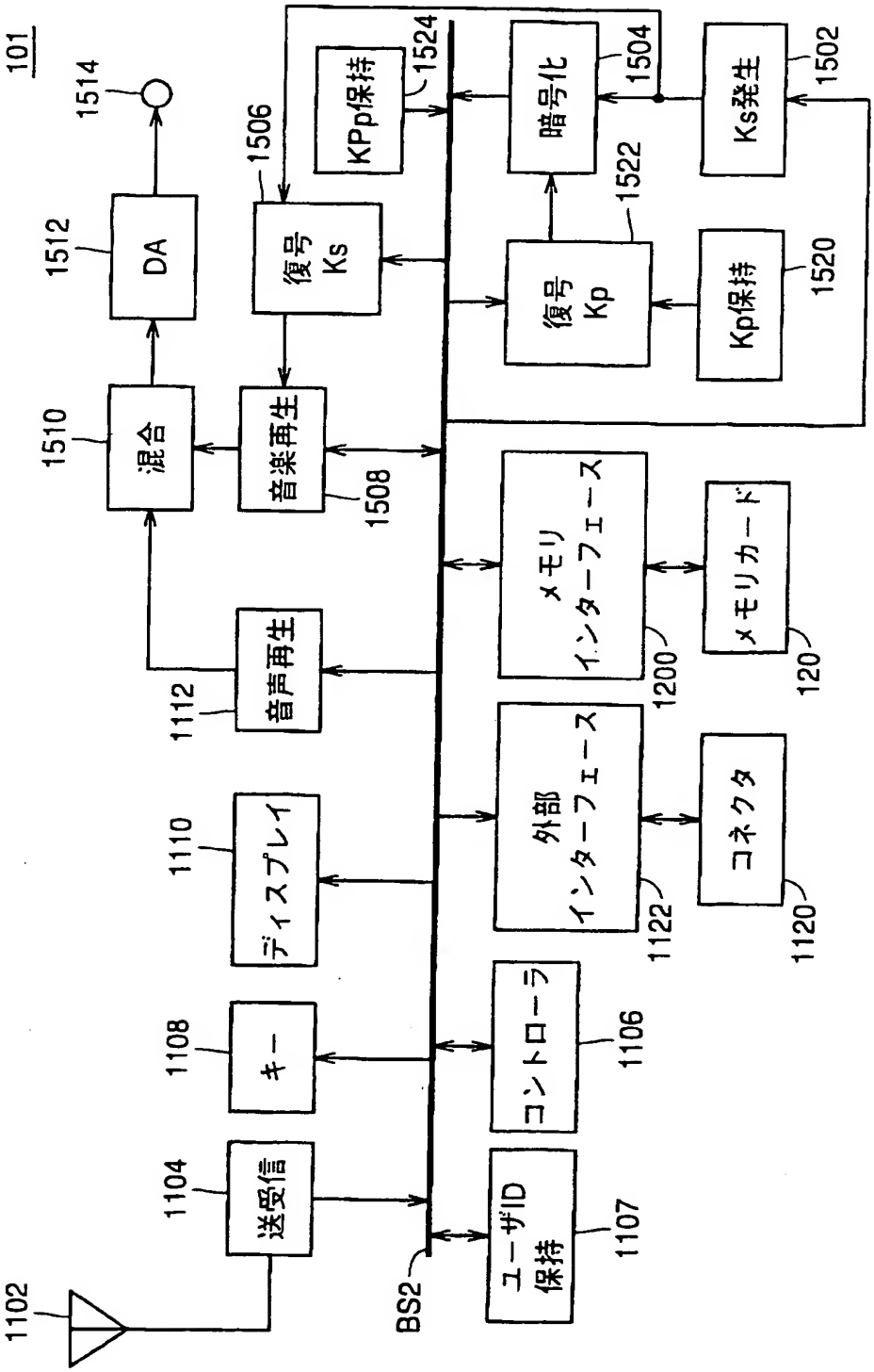

101
1514
1512
DA
1510
混合
1506
復号
Ks
音楽再生
1508
KPp保持
1524
暗号化
1504
Ks発生
1502
1522
復号
Kp
Kp保持
1520
メモリ
インターフェース
1200
メモリカード
120
1112
音声再生
1110
ディスプレイ
外部
インターフェース
1122
コネクタ
1120
1108
キー
コントローラ
1106
1104
送受信
ユーザID
保持
1107
1102
BS2

FIG.12

FIG.13

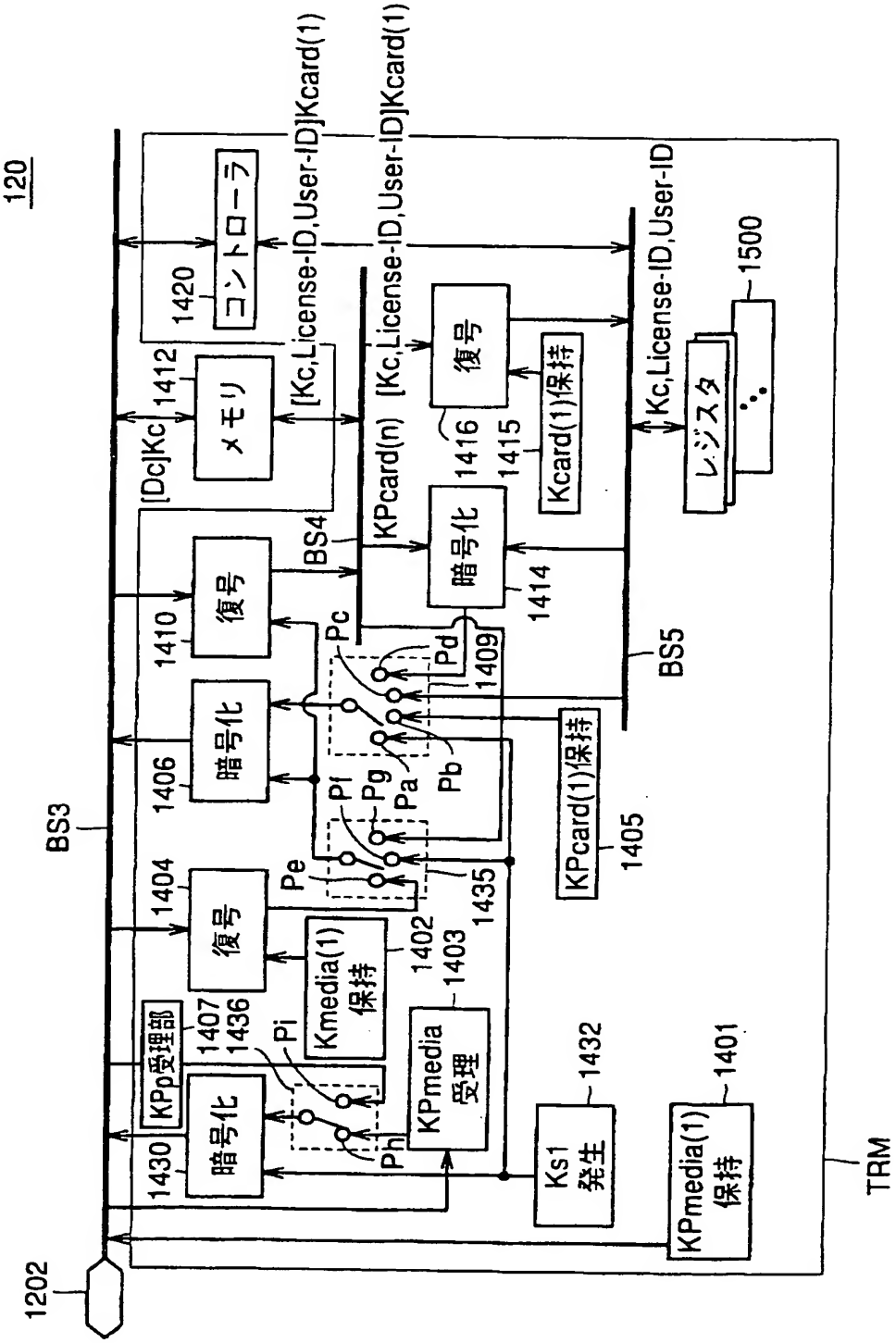

120
1202
BS3
BS4
BS5
TRM
[Dc]Kc
[Kc,License-ID,User-ID]Kcard(1)
[Kc,License-ID,User-ID]Kcard(n)
Kc,License-ID,User-ID
KPcard(n)
KPcard(1)保持
Kcard(1)保持
Kmedia(1)保持
KPmedia(1)保持
KPmedia受理
KPp受理部
Ks1発生
コントローラ
メモリ
レジスタ
暗号化
復号
Pa
Pb
Pc
Pd
Pe
Pf
Pg
Ph
Pi
1400
1401
1402
1403
1404
1405
1406
1407
1409
1410
1412
1414
1415
1416
1420
1430
1432
1435
1436
1500

FIG. 14

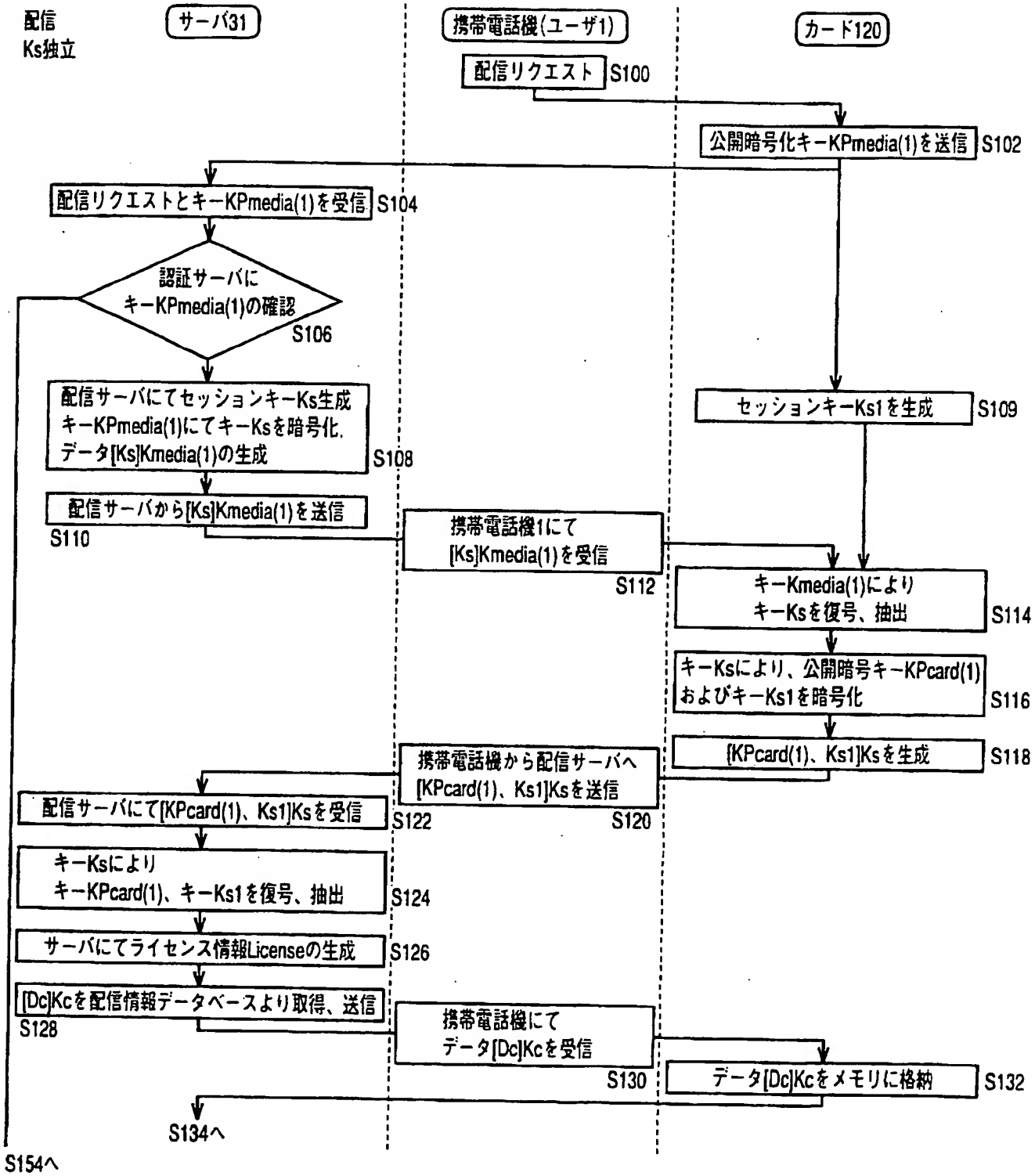

配信
Ks独立
サーバ31
携帯電話機(ユーザ1)
カード120
配信リクエスト S100
公開暗号化キーKPmedia(1)を送信 S102
配信リクエストとキーKPmedia(1)を受信 S104
認証サーバに
キーKPmedia(1)の確認
S106
配信サーバにてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化,
データ[Ks]Kmedia(1)の生成 S108
セッションキーKs1を生成 S109
配信サーバから[Ks]Kmedia(1)を送信
S110
携帯電話機1にて
[Ks]Kmedia(1)を受信
S112
キーKmedia(1)により
キーKsを復号、抽出 S114
キーKsにより、公開暗号キーKPcard(1)
およびキーKs1を暗号化 S116
[KPcard(1)、Ks1]Ksを生成 S118
携帯電話機から配信サーバへ
[KPcard(1)、Ks1]Ksを送信
S120
配信サーバにて[KPcard(1)、Ks1]Ksを受信
S122
キーKsにより
キーKPcard(1)、キーKs1を復号、抽出 S124
サーバにてライセンス情報Licenseの生成 S126
[Dc]Kcを配信情報データベースより取得、送信
S128
携帯電話機にて
データ[Dc]Kcを受信
S130
データ[Dc]Kcをメモリに格納 S132
S134へ
S154へ

FIG.15

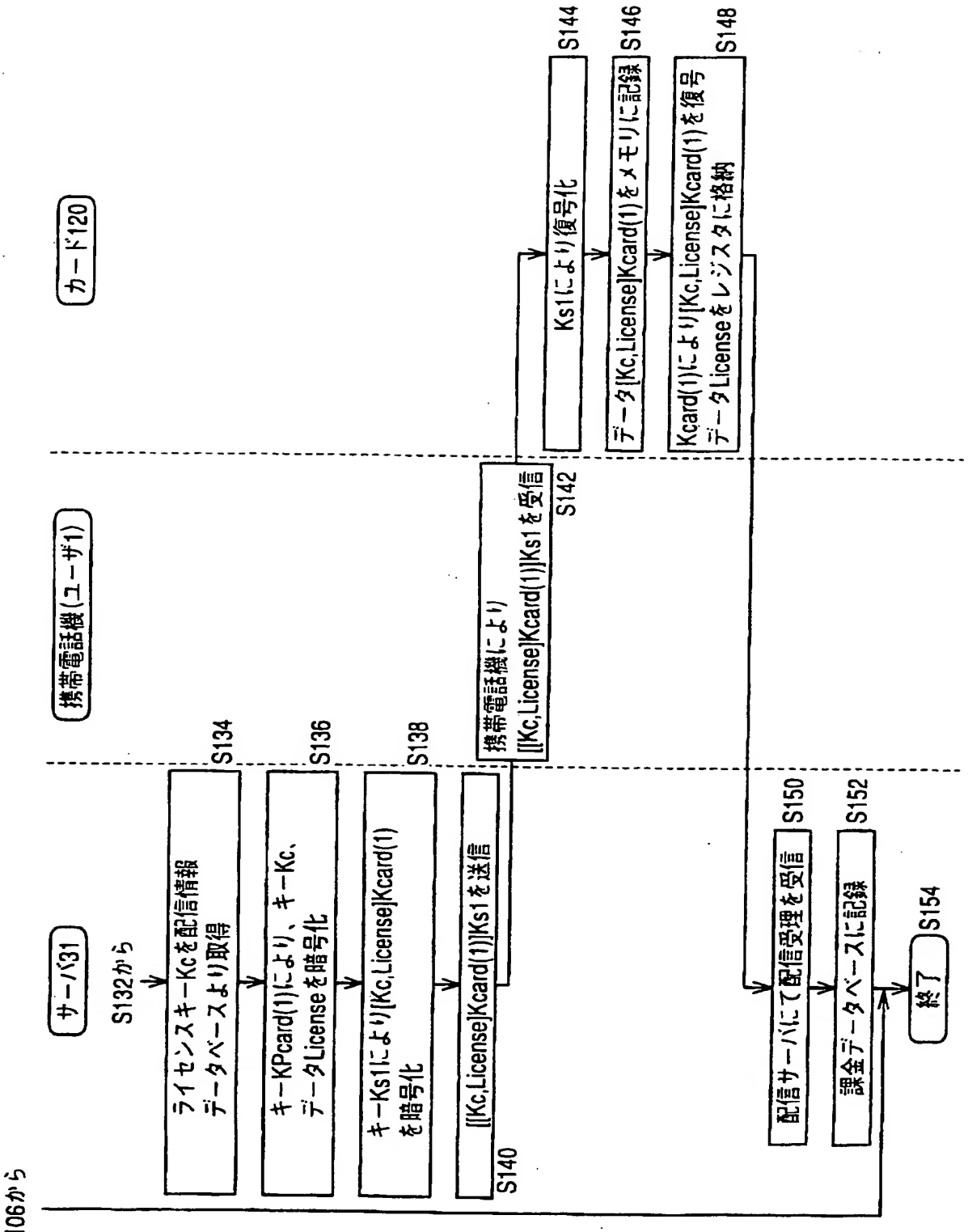

S106から
サーバ31
携帯電話機(ユーザ1)
カード120
S132から
ライセンスキーKcを配信情報データベースより取得
S134
キーKPcard(1)により、キーKc、データLicenseを暗号化
S136
キーKs1により[Kc,License]Kcard(1)を暗号化
S138
[[Kc,License]Kcard(1)]Ks1を送信
S140
携帯電話機により[[Kc,License]Kcard(1)]Ks1を受信
S142
Ks1により復号化
S144
データ[Kc,License]Kcard(1)をメモリに記録
S146
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S148
配信サーバにて配信受理を受信
S150
課金データベースに記録
S152
終了
S154

FIG.16

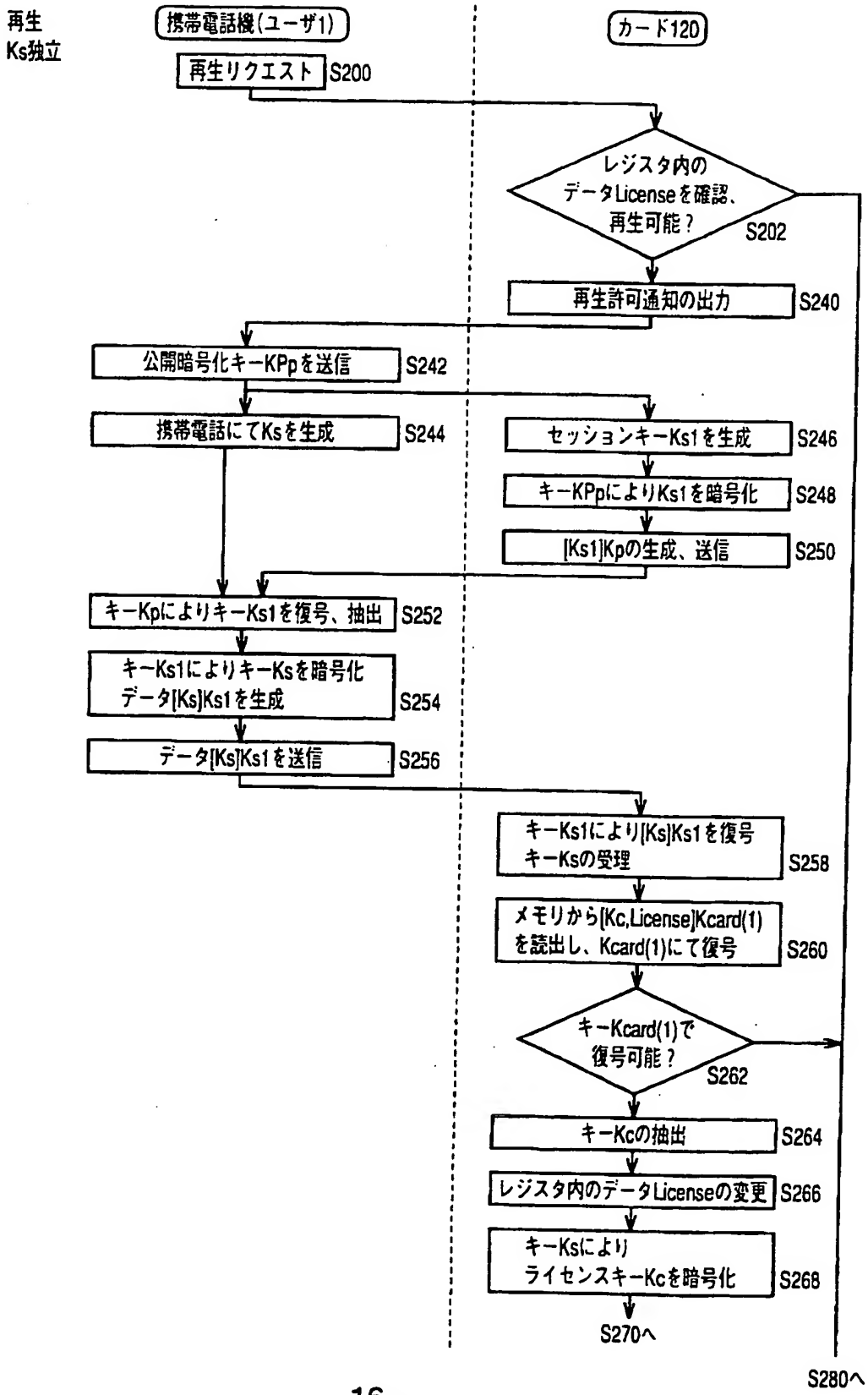

再生
Ks独立
携帯電話機(ユーザ1)
カード120
再生リクエスト S200
レジスタ内のデータLicenseを確認、再生可能？ S202
再生許可通知の出力 S240
公開暗号化キーKPpを送信 S242
携帯電話にてKsを生成 S244
セッションキーKs1を生成 S246
キーKPpによりKs1を暗号化 S248
[Ks1]Kpの生成、送信 S250
キーKpによりキーKs1を復号、抽出 S252
キーKs1によりキーKsを暗号化データ[Ks]Ks1を生成 S254
データ[Ks]Ks1を送信 S256
キーKs1により[Ks]Ks1を復号キーKsの受理 S258
メモリから[Kc,License]Kcard(1)を読出し、Kcard(1)にて復号 S260
キーKcard(1)で復号可能？ S262
キーKcの抽出 S264
レジスタ内のデータLicenseの変更 S266
キーKsによりライセンスキーKcを暗号化 S268
S270へ
S280へ

FIG.17

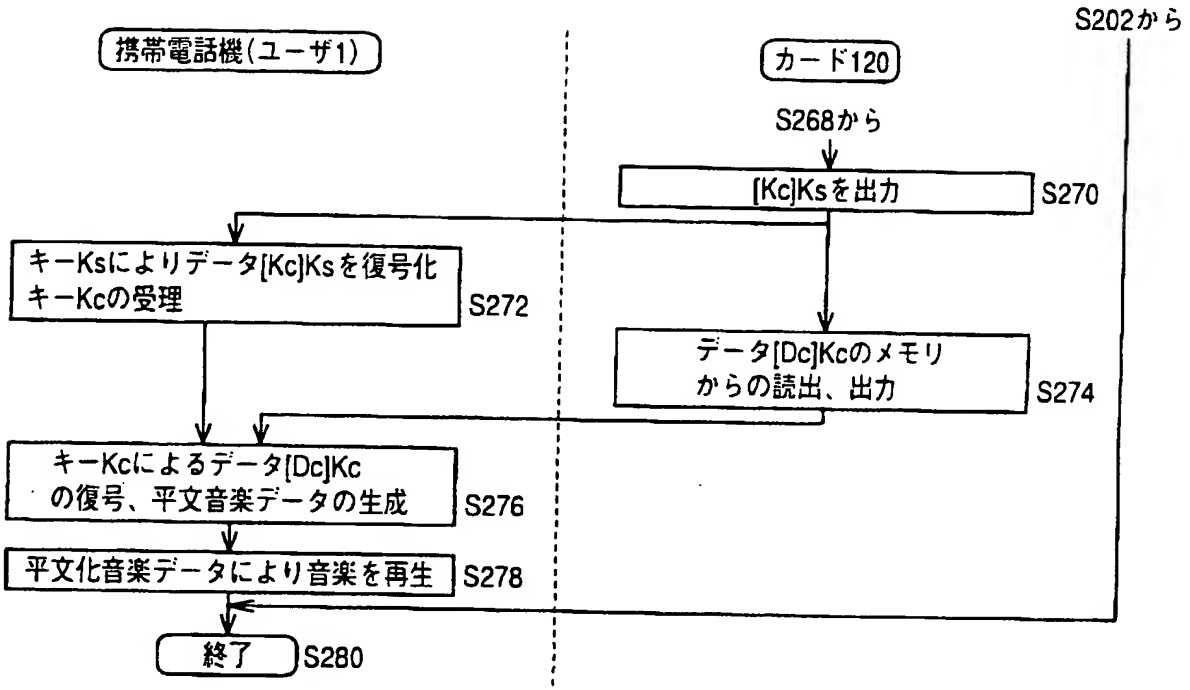

携帯電話機(ユーザ1)
カード120
S202から
S268から
[Kc]Ksを出力
S270
キーKsによりデータ[Kc]Ksを復号化
キーKcの受理
S272
データ[Dc]Kcのメモリ
からの読出、出力
S274
キーKcによるデータ[Dc]Kc
の復号、平文音楽データの生成
S276
平文化音楽データにより音楽を再生
S278
終了
S280

FIG.18

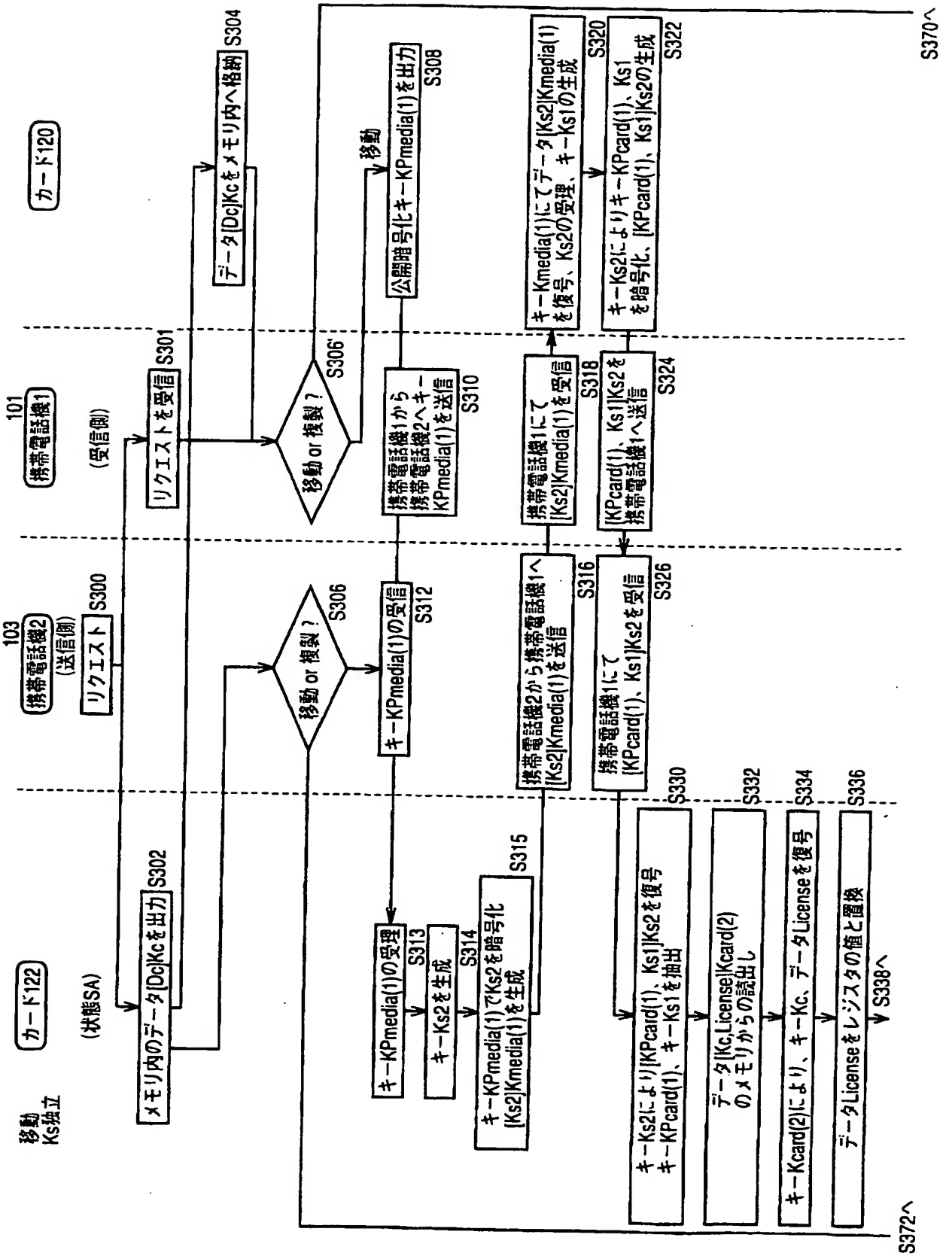
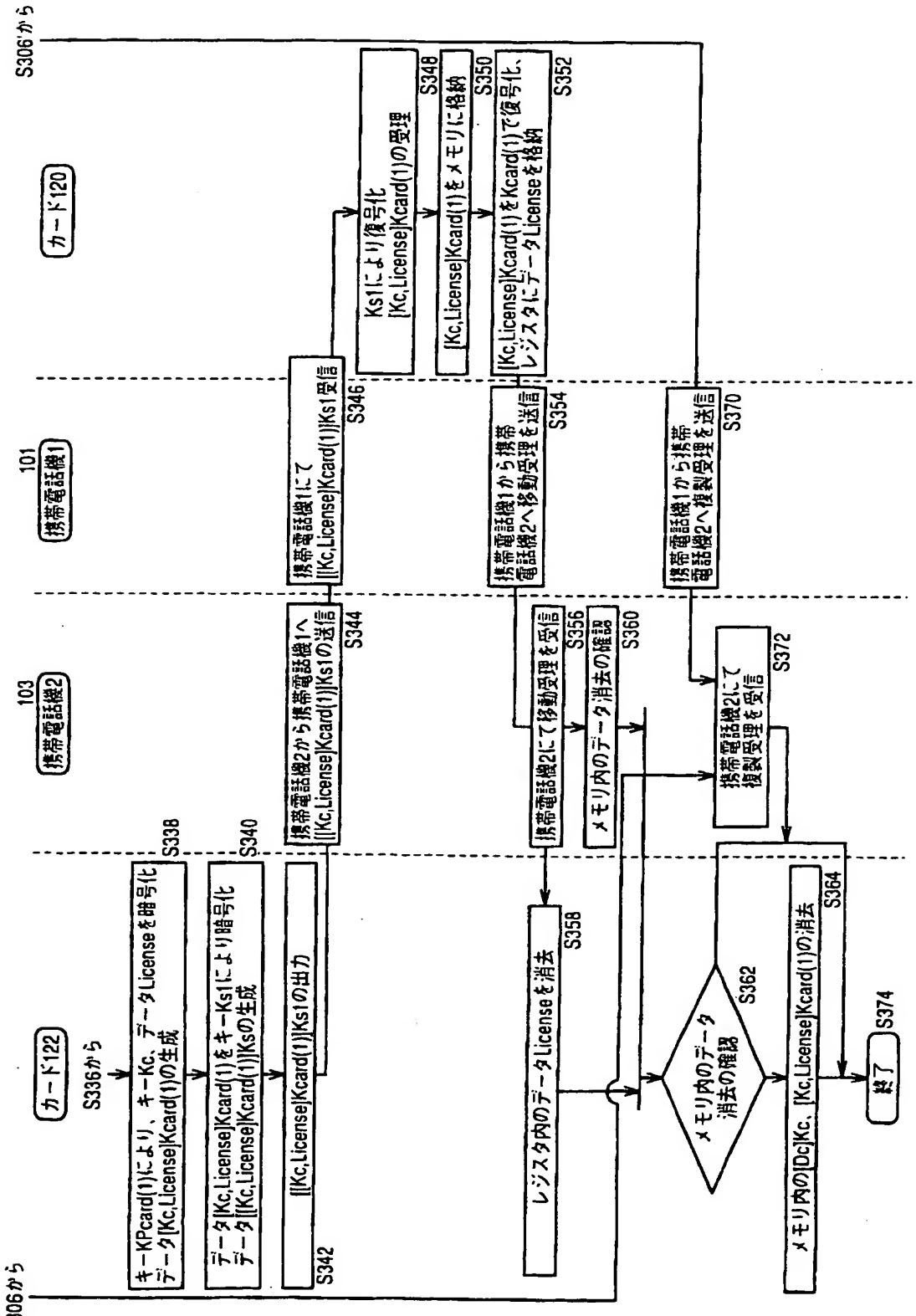

移動
Ks独立
カード122
(状態SA)
メモリ内のデータ[Dc]Kcを出力 S302
103
携帯電話機2
(送信側)
リクエスト S300
101
携帯電話機1
(受信側)
リクエストを受信 S301
カード120
データ[Dc]Kcをメモリ内へ格納 S304
移動 or 複製? S306
移動 or 複製? S306'
キーKPmedia(1)の受理 S313
キーKs2を生成 S314
キーKPmedia(1)でKs2を暗号化 [Ks2]Kmedia(1)を生成 S315
キーKPmedia(1)の受信 S312
公開暗号化キーKPmedia(1)を出力 S308
移動
携帯電話機1から携帯電話機2へキーKPmedia(1)を送信 S310
携帯電話機2から携帯電話機1へ[Ks2]Kmedia(1)を送信 S316
携帯電話機1にて[Ks2]Kmedia(1)を受信 S318
キーKmedia(1)にてデータ[Ks2]Kmedia(1)を復号、Ks2の受理、キーKs1の生成 S320
キーKs2によりキーKPcard(1)、Ks1を暗号化、[KPcard(1)、Ks1]Ks2の生成 S322
[KPcard(1)、Ks1]Ks2を携帯電話機1へ送信 S324
携帯電話機1にて[KPcard(1)、Ks1]Ks2を受信 S326
キーKs2により[KPcard(1)、Ks1]Ks2を復号 キーKPcard(1)、キーKs1を抽出 S330
データ[Kc,License]Kcard(2)のメモリからの読出し S332
キーKcard(2)により、キーKc、データLicenseを復号 S334
データLicenseをレジスタの値と置換 S336
S338へ
S370へ
S372へ

FIG.19


S306から
カード122
103 携帯電話機2
101 携帯電話機1
カード120
S336から
キーKPcard(1)により、キーKc、データLicenseを暗号化 データ[Kc,License]Kcard(1)の生成
S338
データ[Kc,License]Kcard(1)をキーKs1により暗号化 データ[[Kc,License]Kcard(1)]Ksの生成
S340
[[Kc,License]Kcard(1)]Ks1の出力
S342
携帯電話機2から携帯電話機1へ [[Kc,License]Kcard(1)]Ks1の送信
S344
携帯電話機1にて [[Kc,License]Kcard(1)]Ks1受信
S346
Ks1により復号化 [Kc,License]Kcard(1)の受理
S348
[Kc,License]Kcard(1)をメモリに格納
S350
[Kc,License]Kcard(1)をKcard(1)で復号化、レジスタにデータLicenseを格納
S352
携帯電話機1から携帯電話機2へ移動受理を送信
S354
携帯電話機2にて移動受理を受信
S356
メモリ内のデータ消去の確認
S360
携帯電話機1から携帯電話機2へ複製受理を送信
S370
携帯電話機2にて複製受理を受信
S372
レジスタ内のデータLicenseを消去
S358
メモリ内のデータ消去の確認
S362
メモリ内の[Dc]Kc、[Kc,License]Kcard(1)の消去
S364
終了
S374

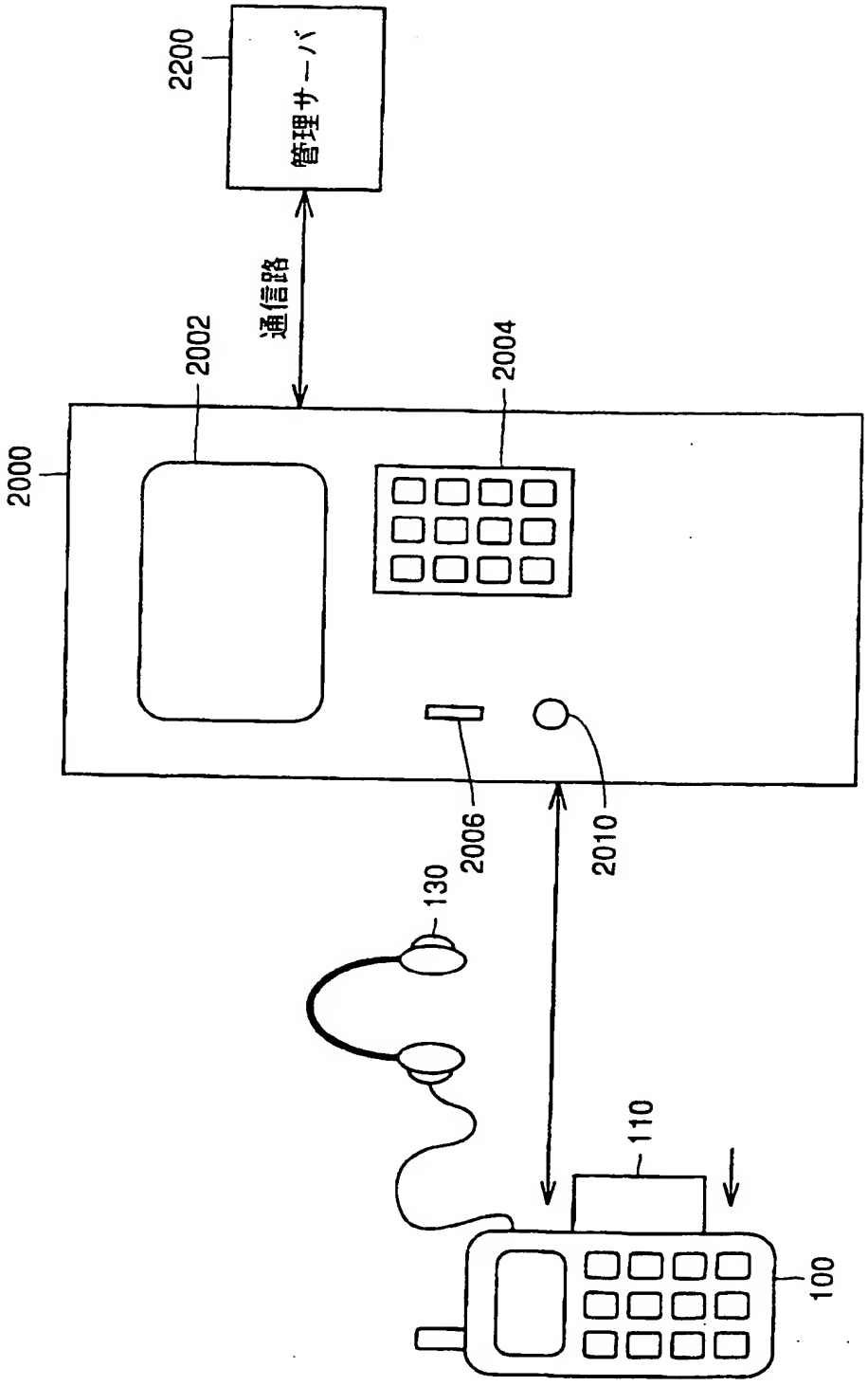


FIG.20

FIG.21

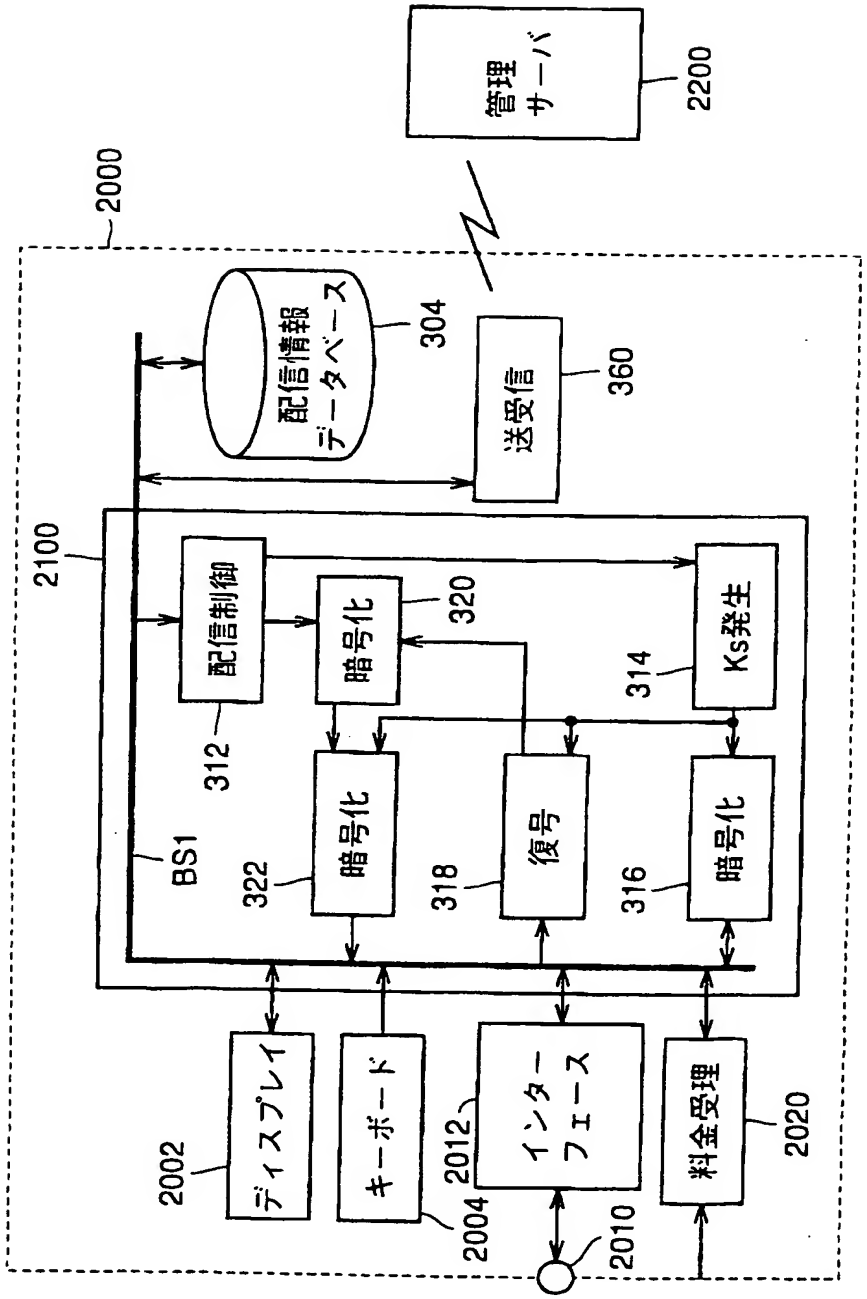

管理サーバ
2200
2000
配信情報データベース
304
送受信
360
2100
配信制御
312
暗号化
320
Ks発生
314
BS1
暗号化
322
復号
318
暗号化
316
ディスプレイ
2002
キーボード
2004
インターフェース
2012
2010
料金受理
2020

FIG.22

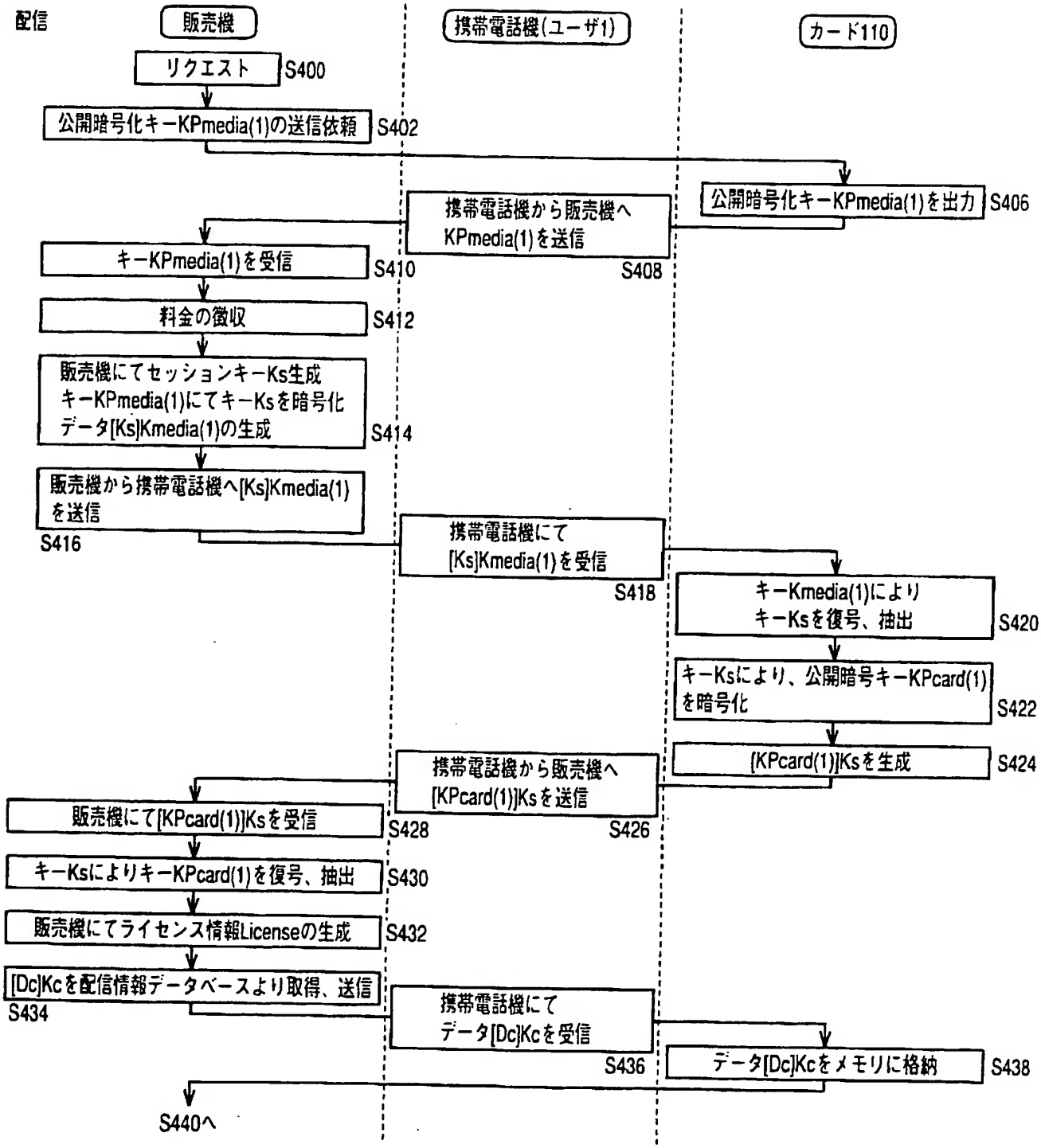
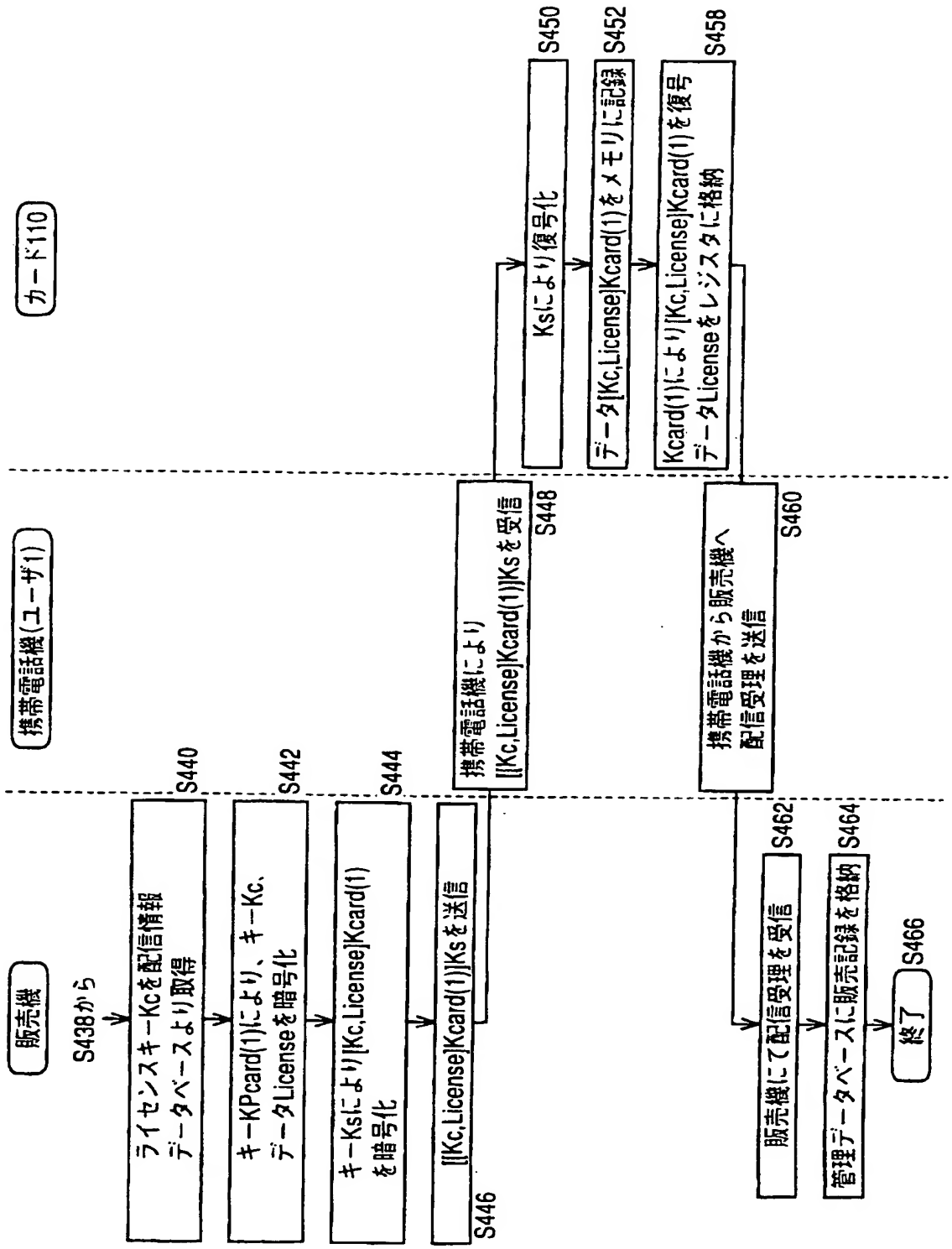

配信
販売機
携帯電話機(ユーザ1)
カード110
リクエスト
S400
公開暗号化キーKPmedia(1)の送信依頼
S402
公開暗号化キーKPmedia(1)を出力
S406
携帯電話機から販売機へ
KPmedia(1)を送信
S408
キーKPmedia(1)を受信
S410
料金の徴収
S412
販売機にてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成
S414
販売機から携帯電話機へ[Ks]Kmedia(1)
を送信
S416
携帯電話機にて
[Ks]Kmedia(1)を受信
S418
キーKmedia(1)により
キーKsを復号、抽出
S420
キーKsにより、公開暗号キーKPcard(1)
を暗号化
S422
[KPcard(1)]Ksを生成
S424
携帯電話機から販売機へ
[KPcard(1)]Ksを送信
S426
販売機にて[KPcard(1)]Ksを受信
S428
キーKsによりキーKPcard(1)を復号、抽出
S430
販売機にてライセンス情報Licenseの生成
S432
[Dc]Kcを配信情報データベースより取得、送信
S434
携帯電話機にて
データ[Dc]Kcを受信
S436
データ[Dc]Kcをメモリに格納
S438
S440へ

FIG.23


販売機
携帯電話機(ユーザ1)
カード110
S438から
ライセンスキーKcを配信情報データベースより取得
S440
キーKPcard(1)により、キーKc、データLicenseを暗号化
S442
キーKsにより[Kc,License]Kcard(1)を暗号化
S444
[[Kc,License]Kcard(1)]Ksを送信
S446
携帯電話機により[[Kc,License]Kcard(1)]Ksを受信
S448
Ksにより復号化
S450
データ[Kc,License]Kcard(1)をメモリに記録
S452
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S458
携帯電話機から販売機へ配信受理を送信
S460
販売機にて配信受理を受信
S462
管理データベースに販売記録を格納
S464
終了
S466

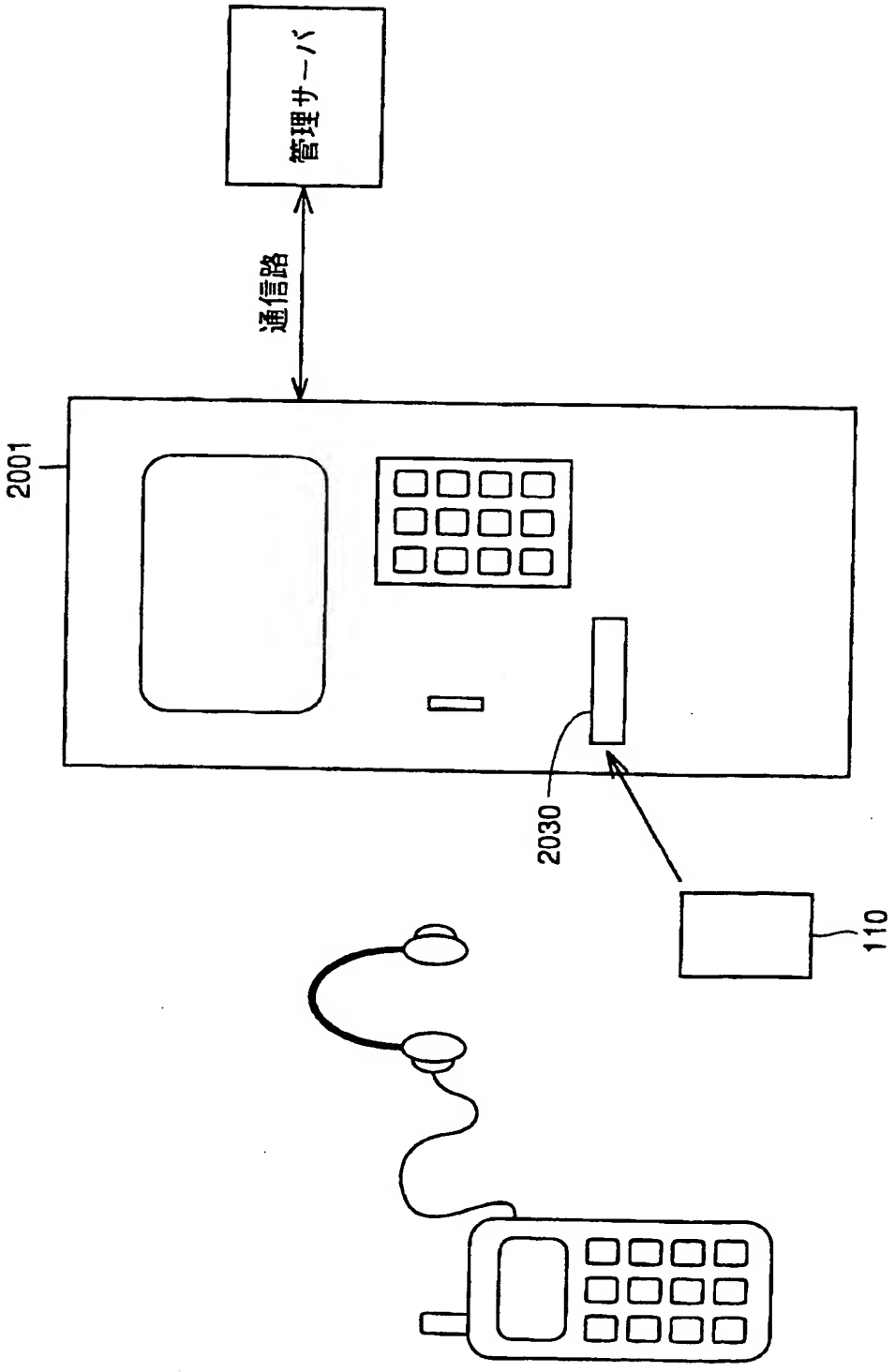


FIG.24

FIG.25

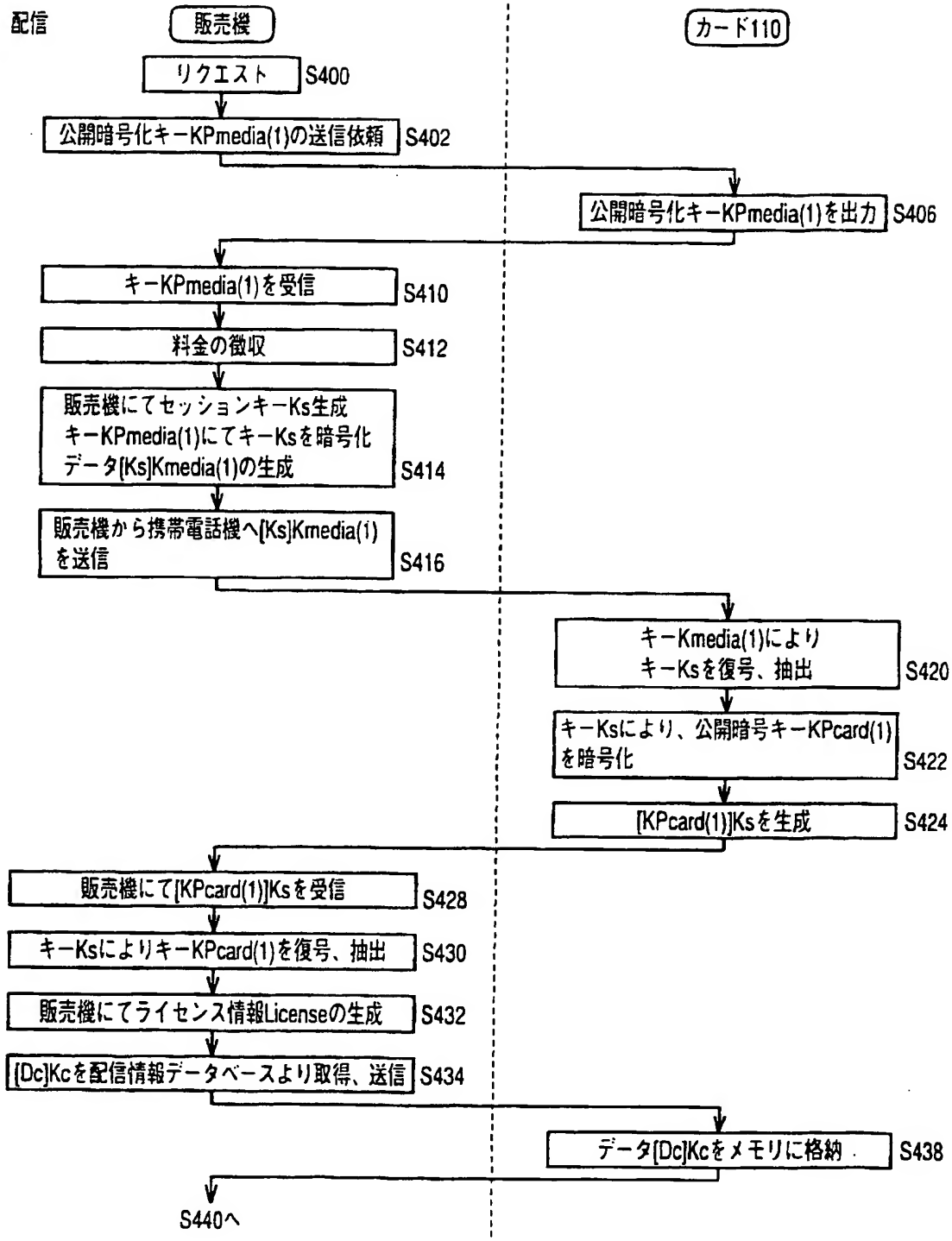
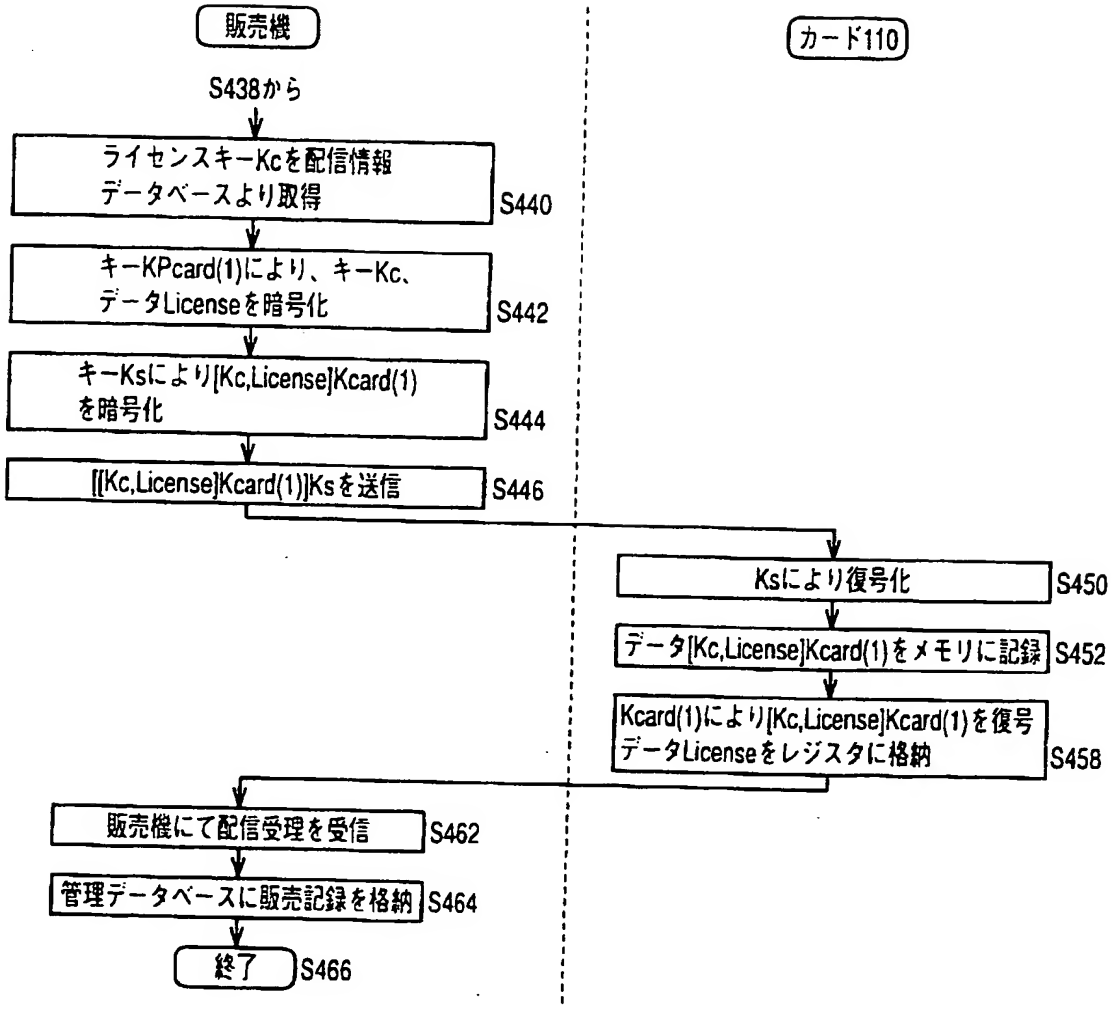

配信
販売機
カード110
リクエスト
S400
公開暗号化キーKPmedia(1)の送信依頼
S402
公開暗号化キーKPmedia(1)を出力
S406
キーKPmedia(1)を受信
S410
料金の徴収
S412
販売機にてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成
S414
販売機から携帯電話機へ[Ks]Kmedia(1)
を送信
S416
キーKmedia(1)により
キーKsを復号、抽出
S420
キーKsにより、公開暗号キーKPcard(1)
を暗号化
S422
[KPcard(1)]Ksを生成
S424
販売機にて[KPcard(1)]Ksを受信
S428
キーKsによりキーKPcard(1)を復号、抽出
S430
販売機にてライセンス情報Licenseの生成
S432
[Dc]Kcを配信情報データベースより取得、送信
S434
データ[Dc]Kcをメモリに格納
S438
S440へ

FIG.26


販売機
カード110
S438から
ライセンスキーKcを配信情報データベースより取得
S440
キーKPcard(1)により、キーKc、データLicenseを暗号化
S442
キーKsにより[Kc,License]Kcard(1)を暗号化
S444
[[Kc,License]Kcard(1)]Ksを送信
S446
Ksにより復号化
S450
データ[Kc,License]Kcard(1)をメモリに記録
S452
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S458
販売機にて配信受理を受信
S462
管理データベースに販売記録を格納
S464
終了
S466

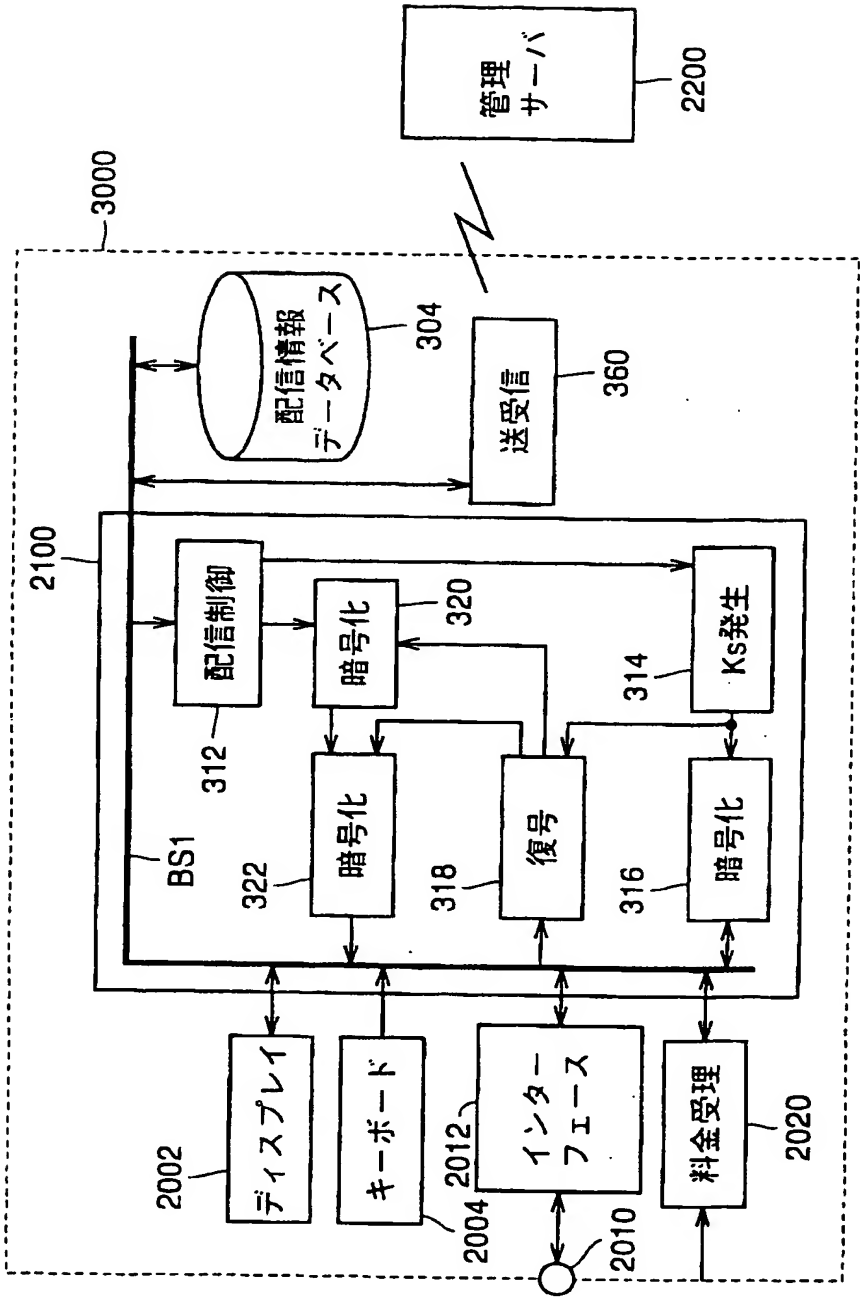

管理サーバ
2200
3000
配信情報データベース
304
送受信
360
2100
配信制御
312
暗号化
320
Ks発生
314
BS1
暗号化
322
復号
318
暗号化
316
ディスプレイ
2002
キーボード
2004
インターフェース
2012
2010
料金受理
2020

FIG.27

FIG.28

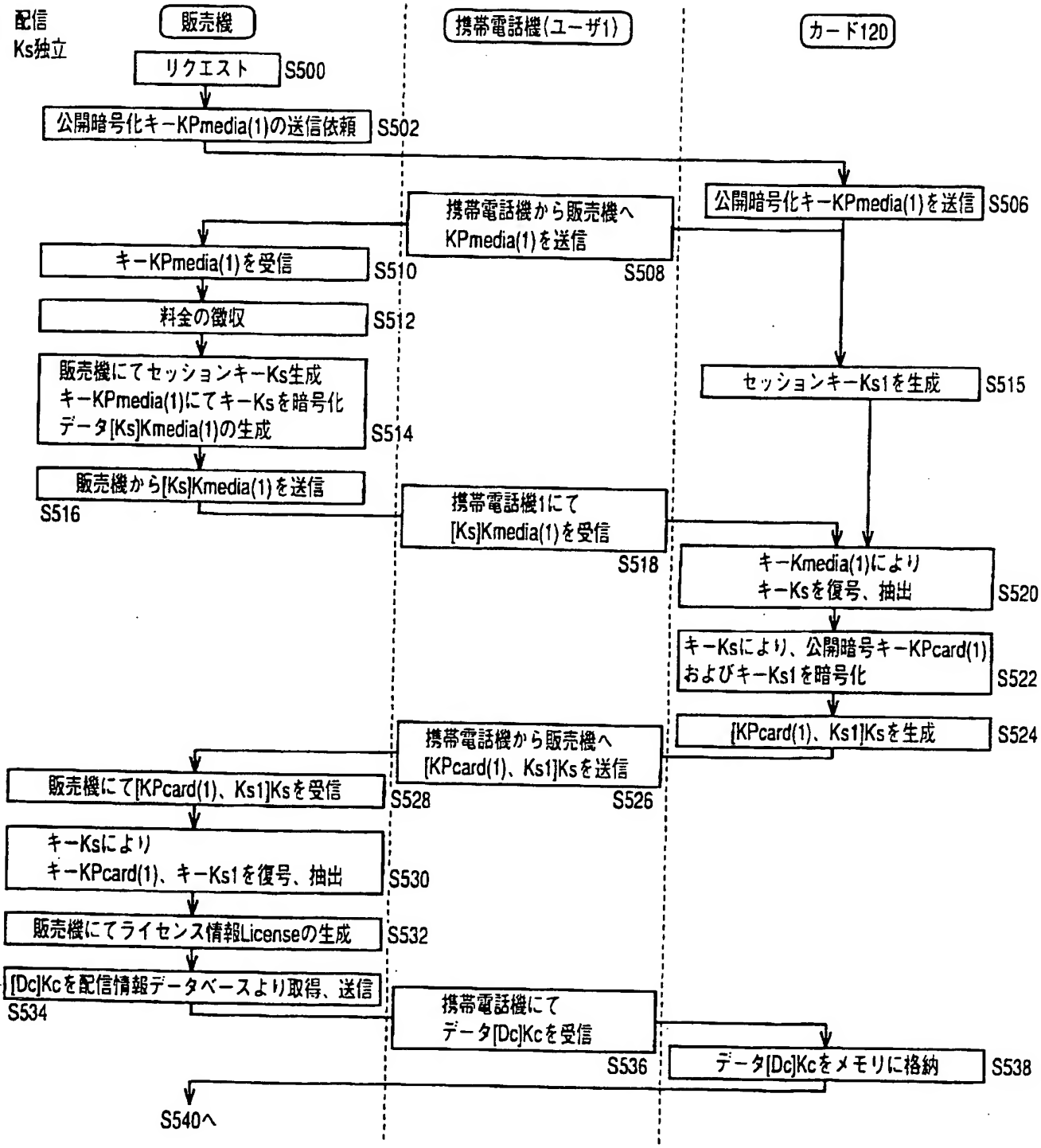

配信
Ks独立
販売機
携帯電話機(ユーザ1)
カード120
リクエスト S500
公開暗号化キーKPmedia(1)の送信依頼 S502
公開暗号化キーKPmedia(1)を送信 S506
携帯電話機から販売機へ
KPmedia(1)を送信
S508
キーKPmedia(1)を受信 S510
料金の徴収 S512
セッションキーKs1を生成 S515
販売機にてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成 S514
販売機から[Ks]Kmedia(1)を送信
S516
携帯電話機1にて
[Ks]Kmedia(1)を受信
S518
キーKmedia(1)により
キーKsを復号、抽出 S520
キーKsにより、公開暗号キーKPcard(1)
およびキーKs1を暗号化 S522
[KPcard(1)、Ks1]Ksを生成 S524
携帯電話機から販売機へ
[KPcard(1)、Ks1]Ksを送信
S526
販売機にて[KPcard(1)、Ks1]Ksを受信
S528
キーKsにより
キーKPcard(1)、キーKs1を復号、抽出 S530
販売機にてライセンス情報Licenseの生成 S532
[Dc]Kcを配信情報データベースより取得、送信
S534
携帯電話機にて
データ[Dc]Kcを受信
S536
データ[Dc]Kcをメモリに格納 S538
S540へ

FIG.29

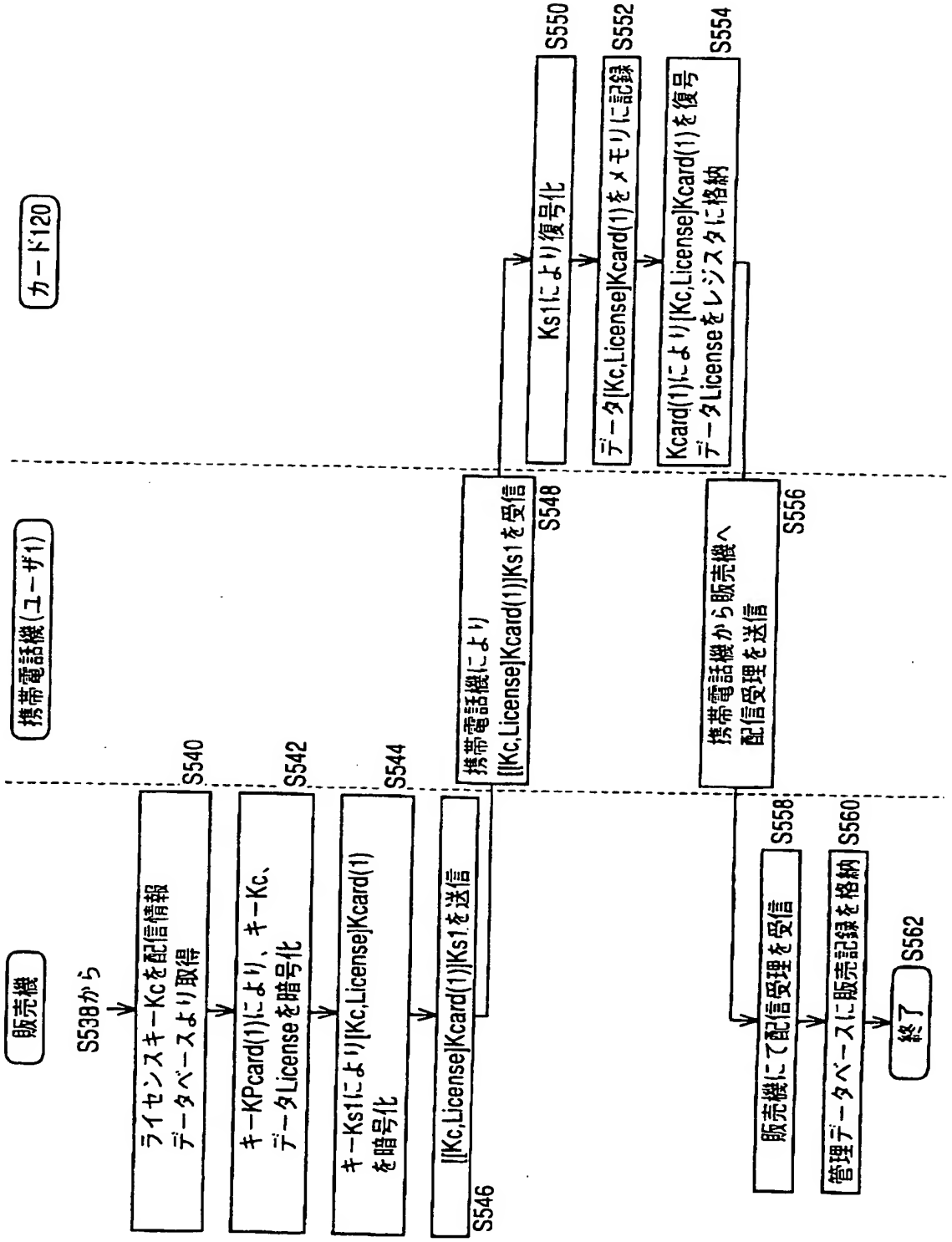

販売機
携帯電話機(ユーザ1)
カード120
S538から
ライセンスキーKcを配信情報データベースより取得
S540
キーKPcard(1)により、キーKc、データLicenseを暗号化
S542
キーKs1により|Kc,License|Kcard(1)を暗号化
S544
|Kc,License|Kcard(1)|Ks1を送信
S546
携帯電話機により|Kc,License|Kcard(1)|Ks1を受信
S548
Ks1により復号化
S550
データ|Kc,License|Kcard(1)をメモリに記録
S552
Kcard(1)により|Kc,License|Kcard(1)を復号データLicenseをレジスタに格納
S554
携帯電話機から販売機へ配信受理を送信
S556
販売機にて配信受理を受信
S558
管理データベースに販売記録を格納
S560
終了
S562

FIG.30

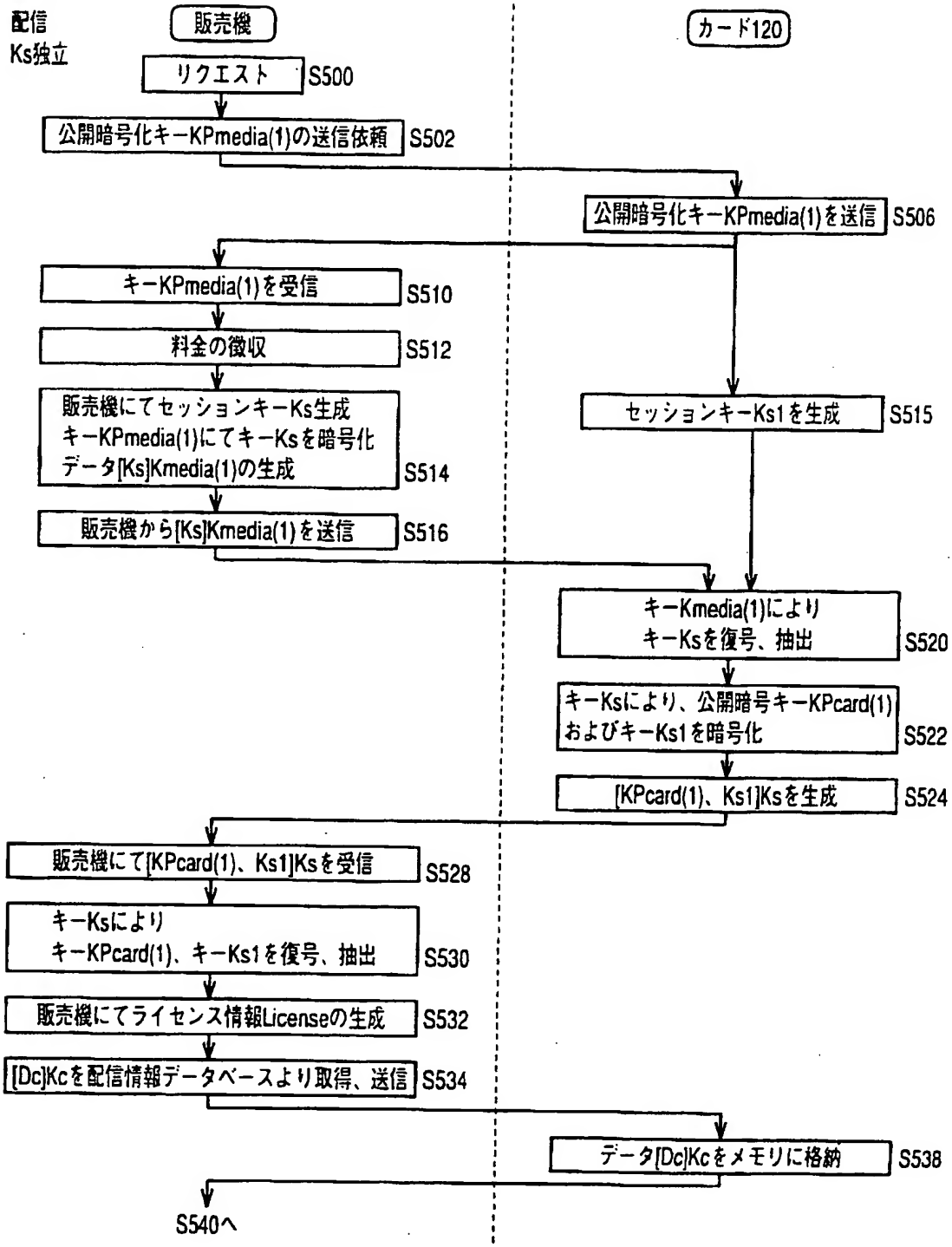

配信
Ks独立
販売機
カード120
リクエスト
S500
公開暗号化キーKPmedia(1)の送信依頼
S502
公開暗号化キーKPmedia(1)を送信
S506
キーKPmedia(1)を受信
S510
料金の徴収
S512
販売機にてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成
S514
セッションキーKs1を生成
S515
販売機から[Ks]Kmedia(1)を送信
S516
キーKmedia(1)により
キーKsを復号、抽出
S520
キーKsにより、公開暗号キーKPcard(1)
およびキーKs1を暗号化
S522
[KPcard(1)、Ks1]Ksを生成
S524
販売機にて[KPcard(1)、Ks1]Ksを受信
S528
キーKsにより
キーKPcard(1)、キーKs1を復号、抽出
S530
販売機にてライセンス情報Licenseの生成
S532
[Dc]Kcを配信情報データベースより取得、送信
S534
データ[Dc]Kcをメモリに格納
S538
S540へ

FIG.31

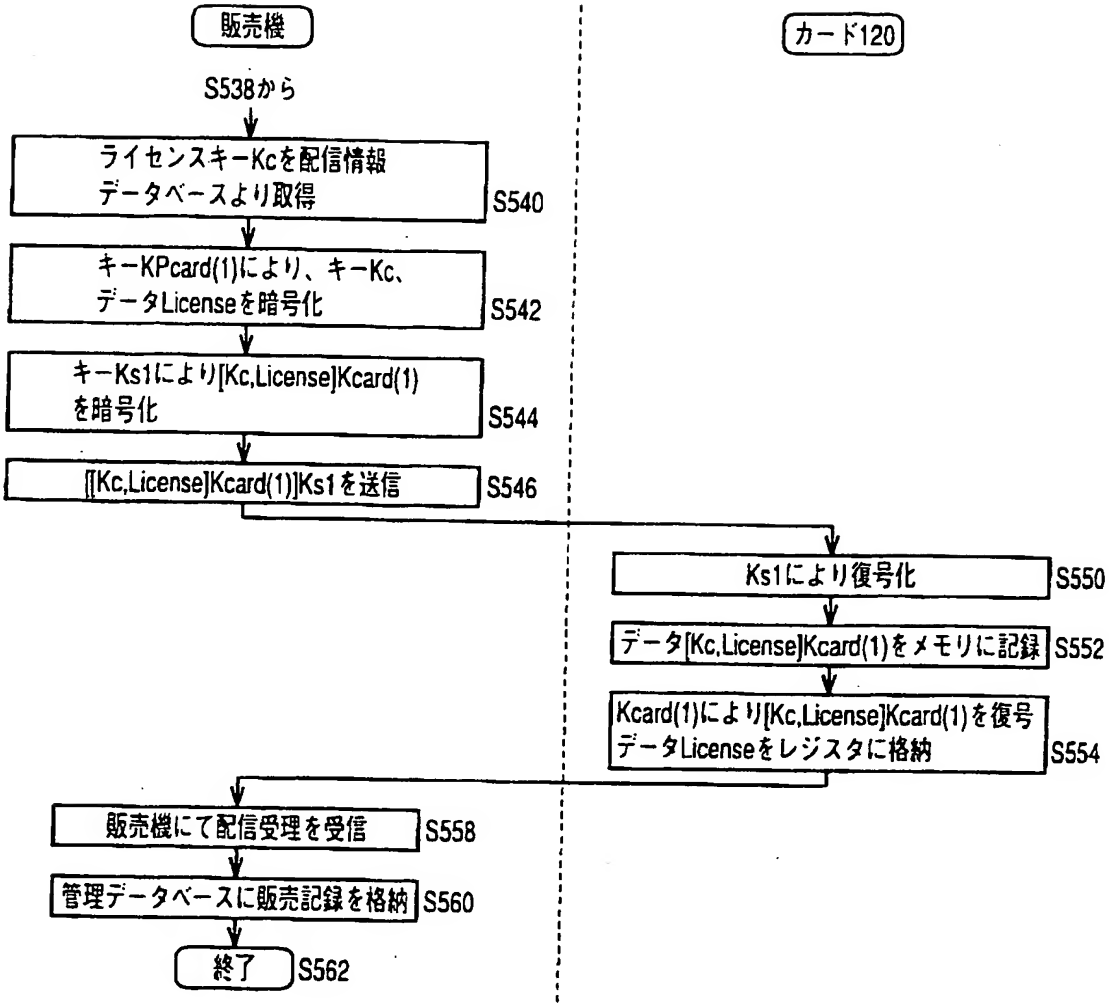
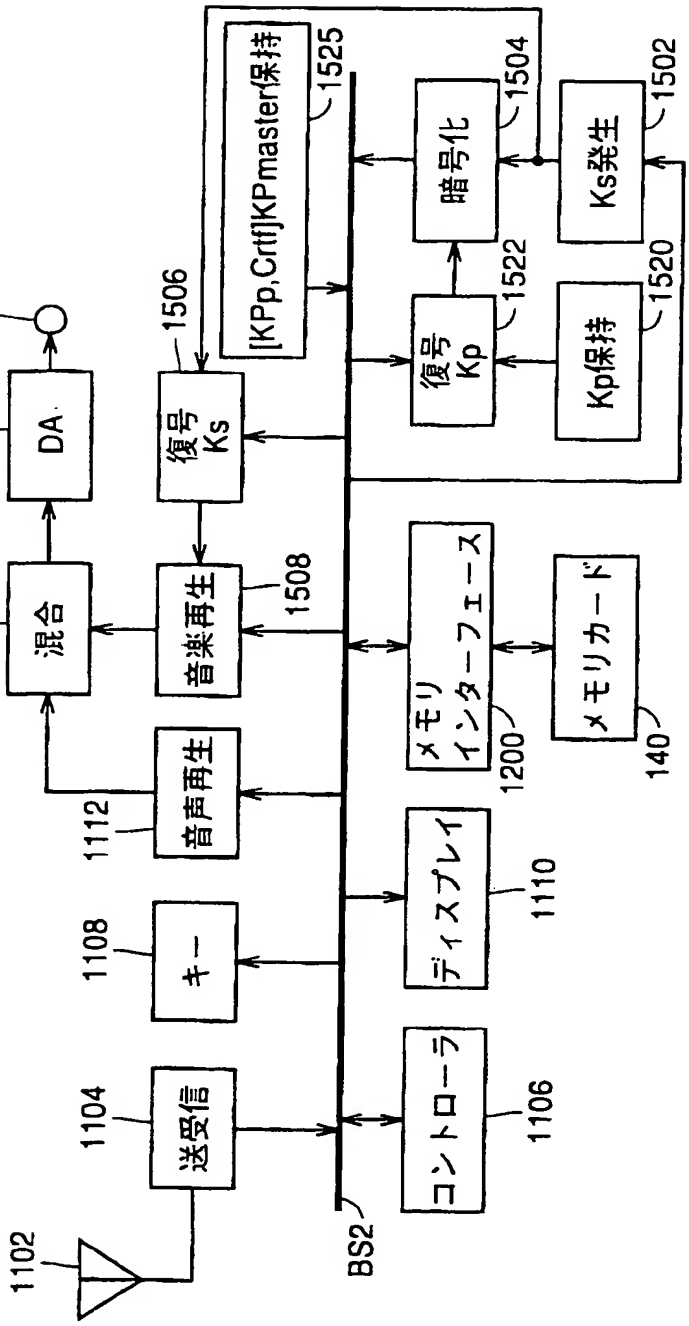

販売機
カード120
S538から
ライセンスキーKcを配信情報データベースより取得
S540
キーKPcard(1)により、キーKc、データLicenseを暗号化
S542
キーKs1により[Kc,License]Kcard(1)を暗号化
S544
[[Kc,License]Kcard(1)]Ks1を送信
S546
Ks1により復号化
S550
データ[Kc,License]Kcard(1)をメモリに記録
S552
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S554
販売機にて配信受理を受信
S558
管理データベースに販売記録を格納
S560
終了
S562

FIG.32


105
1514
1512
DA
1510
混合
1508
音楽再生
1112
音声再生
1108
キー
1104
送受信
1102
1506
復号
Ks
[KPp,CrtfJKPmaster保持
1525
BS2
コントローラ
1106
ディスプレイ
1110
メモリ
インターフェース
1200
メモリカード
140
暗号化
1504
復号
Kp
1522
Kpi保持
1520
Ks発生
1502

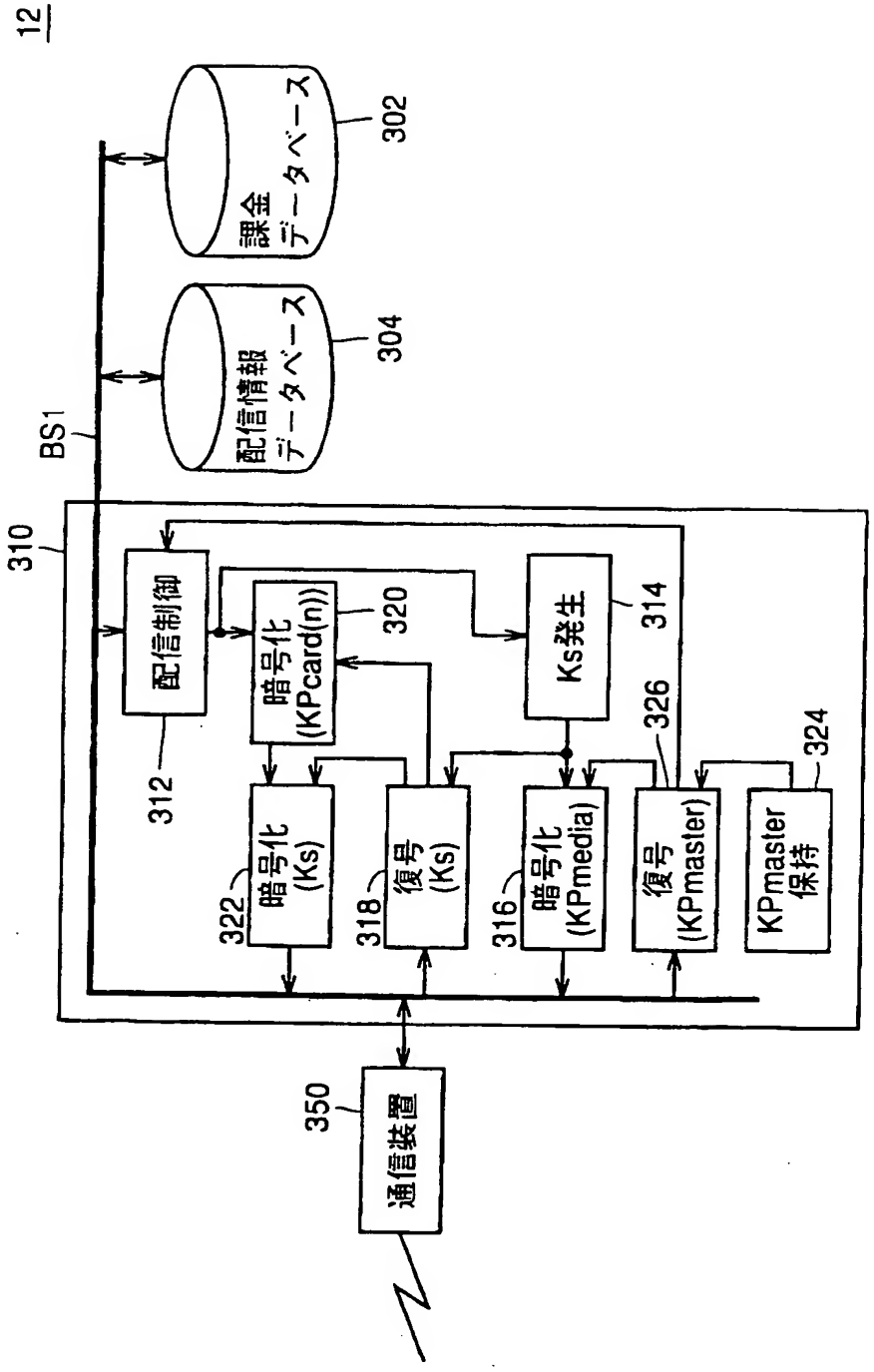

12
課金データベース
302
配信情報データベース
304
BS1
310
配信制御
312
暗号化(KPcard(n))
320
Ks発生
314
暗号化(Ks)
322
復号(Ks)
318
暗号化(KPmedia)
316
復号(KPmaster)
326
KPmaster保持
324
通信装置
350

FIG.33

FIG.34

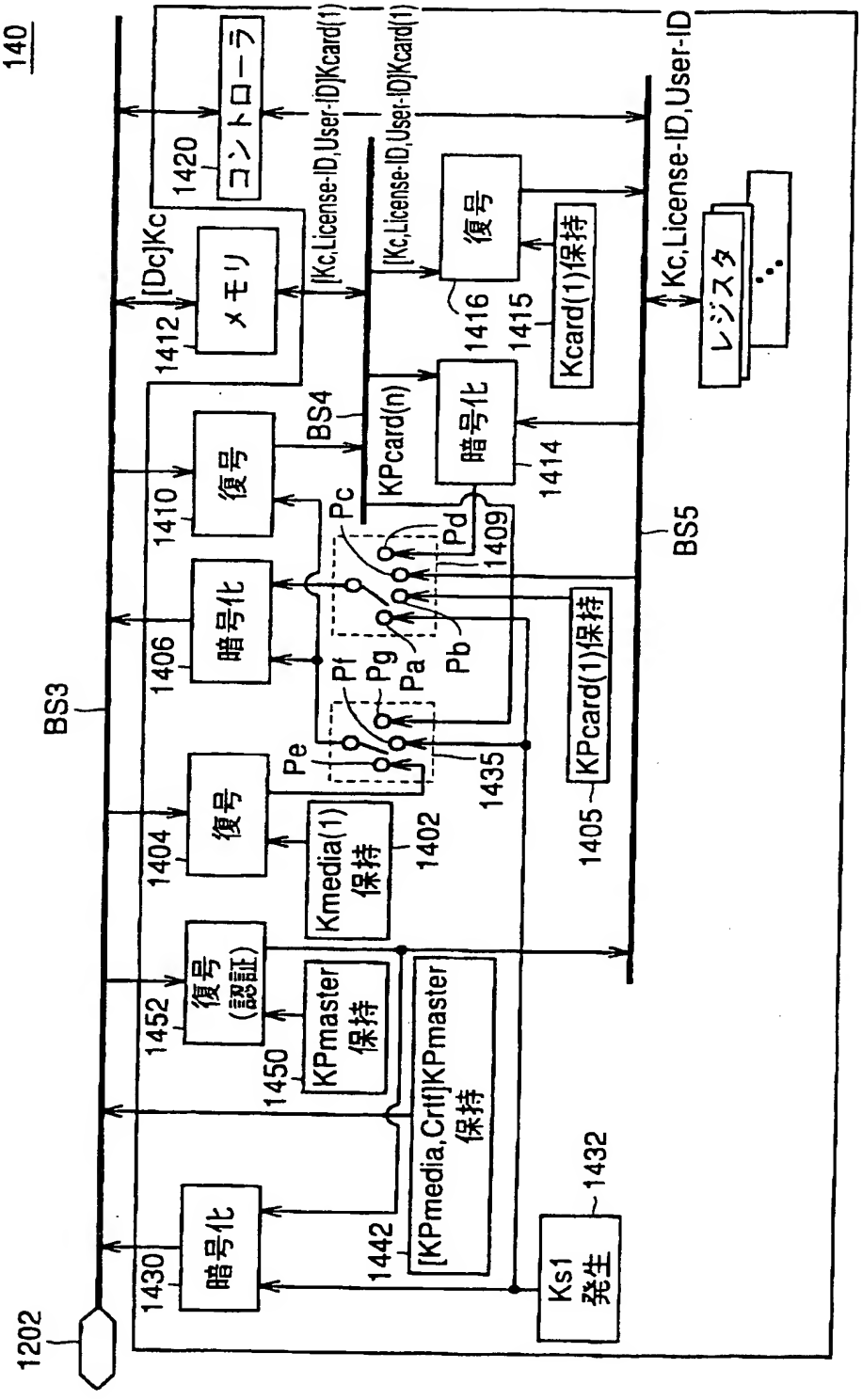

140
1202
BS3
BS4
BS5
1430
暗号化
1442
[KPmedia,Crit]KPmaster
保持
1450
KPmaster
保持
1452
復号
(認証)
1404
復号
1406
暗号化
1410
復号
1412
メモリ
1420
コントローラ
Ks1
発生
1432
Kmedia(1)
保持
1402
Pe
Pf
Pg
Pa
Pb
Pc
Pd
1435
KPcard(n)
1409
1405
KPcard(1)保持
[Dc]Kc
[Kc,License-ID,User-ID]Kcard(1)
[Kc,License-ID,User-ID]Kcard(1)
1414
暗号化
1416
復号
1415
Kcard(1)保持
Kc,License-ID,User-ID
レジスタ

FIG.35

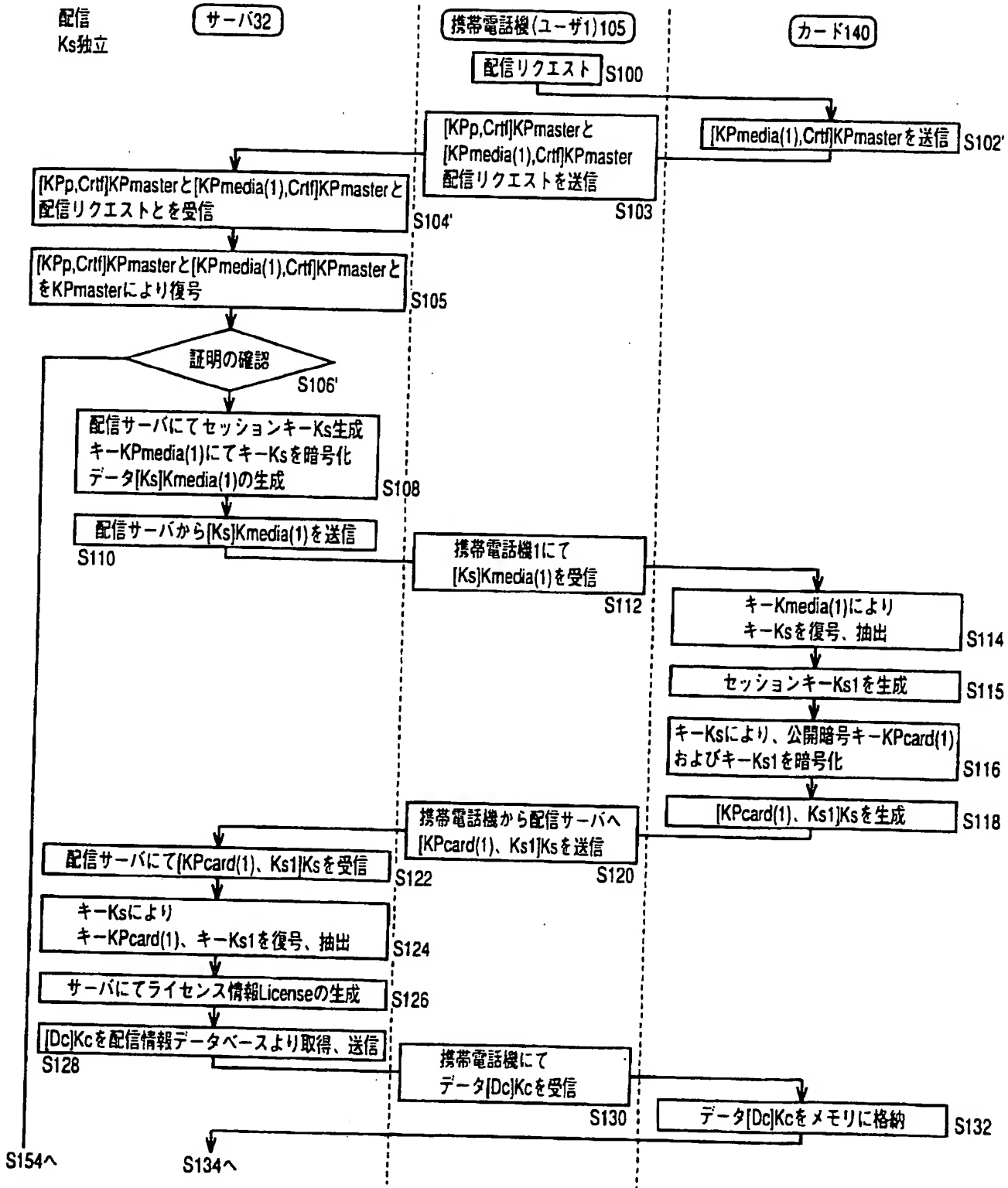

配信
Ks独立
サーバ32
携帯電話機(ユーザ1)105
カード140
配信リクエスト S100
[KPp,Crtf]KPmasterと[KPmedia(1),Crtf]KPmasterを送信 S102'
[KPp,Crtf]KPmasterと[KPmedia(1),Crtf]KPmaster配信リクエストを送信 S103
[KPp,Crtf]KPmasterと[KPmedia(1),Crtf]KPmasterと配信リクエストとを受信 S104'
[KPp,Crtf]KPmasterと[KPmedia(1),Crtf]KPmasterとをKPmasterにより復号 S105
証明の確認 S106'
配信サーバにてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成 S108
配信サーバから[Ks]Kmedia(1)を送信 S110
携帯電話機1にて[Ks]Kmedia(1)を受信 S112
キーKmedia(1)によりキーKsを復号、抽出 S114
セッションキーKs1を生成 S115
キーKsにより、公開暗号キーKPcard(1)およびキーKs1を暗号化 S116
[KPcard(1)、Ks1]Ksを生成 S118
携帯電話機から配信サーバへ[KPcard(1)、Ks1]Ksを送信 S120
配信サーバにて[KPcard(1)、Ks1]Ksを受信 S122
キーKsによりキーKPcard(1)、キーKs1を復号、抽出 S124
サーバにてライセンス情報Licenseの生成 S126
[Dc]Kcを配信情報データベースより取得、送信 S128
携帯電話機にてデータ[Dc]Kcを受信 S130
データ[Dc]Kcをメモリに格納 S132
S154へ
S134へ

FIG.36

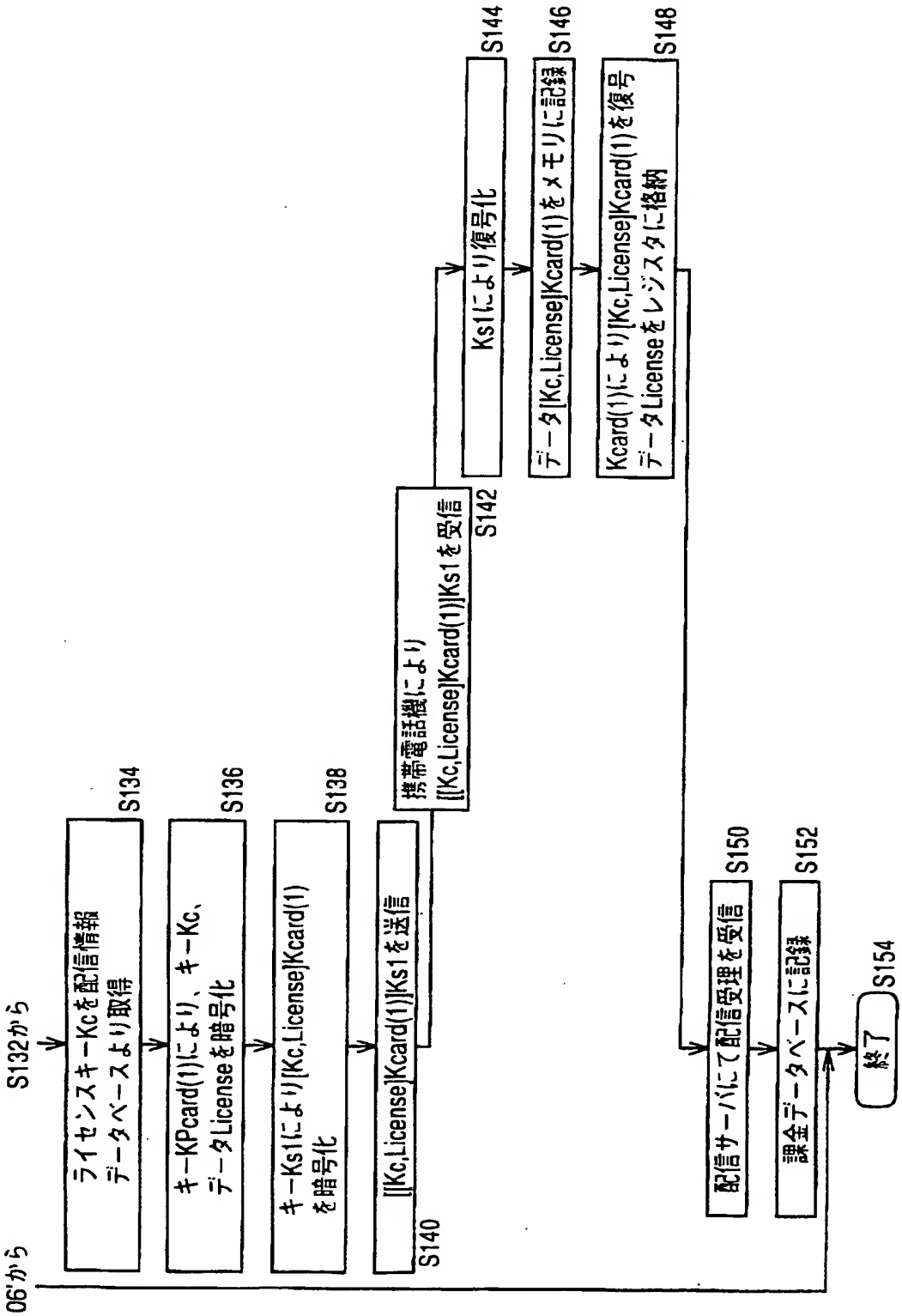

S106'から
S132から
ライセンスキーKcを配信情報データベースより取得
S134
キーKPcard(1)により、キーKc、データLicenseを暗号化
S136
キーKs1により[Kc,License]Kcard(1)を暗号化
S138
[Kc,License]Kcard(1)]Ks1を送信
S140
携帯電話機により[[Kc,License]Kcard(1)]Ks1を受信
S142
Ks1により復号化
S144
データ[Kc,License]Kcard(1)をメモリに記録
S146
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S148
配信サーバにて配信受理を受信
S150
課金データベースに記録
S152
終了
S154

FIG.37

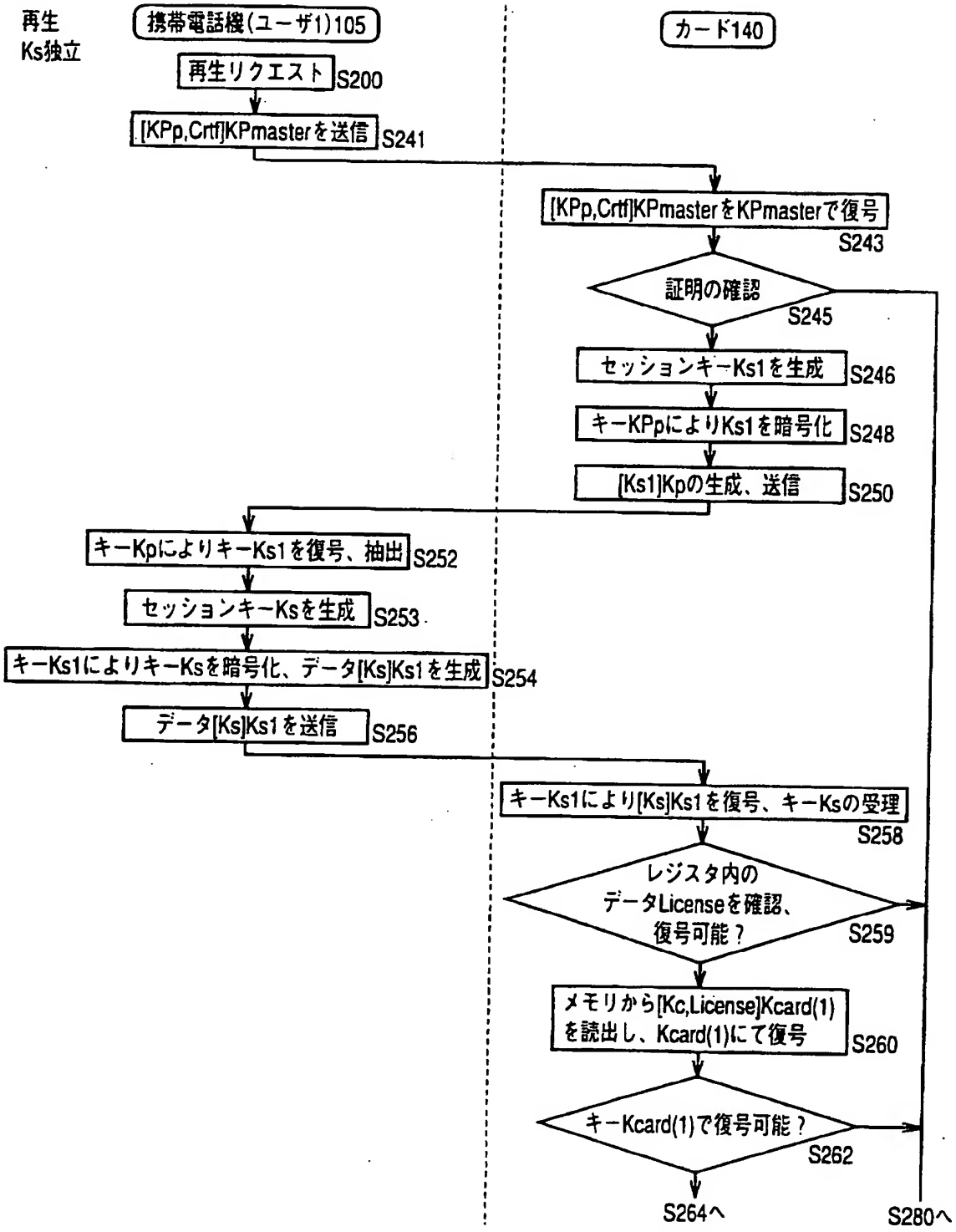

再生
Ks独立
携帯電話機(ユーザ1)105
カード140
再生リクエスト S200
[KPp,Crtf]KPmasterを送信 S241
[KPp,Crtf]KPmasterをKPmasterで復号 S243
証明の確認 S245
セッションキーKs1を生成 S246
キーKPpによりKs1を暗号化 S248
[Ks1]Kpの生成、送信 S250
キーKpによりキーKs1を復号、抽出 S252
セッションキーKsを生成 S253
キーKs1によりキーKsを暗号化、データ[Ks]Ks1を生成 S254
データ[Ks]Ks1を送信 S256
キーKs1により[Ks]Ks1を復号、キーKsの受理 S258
レジスタ内の
データLicenseを確認、
復号可能？ S259
メモリから[Kc,License]Kcard(1)
を読出し、Kcard(1)にて復号 S260
キーKcard(1)で復号可能？ S262
S264へ
S280へ

FIG.38

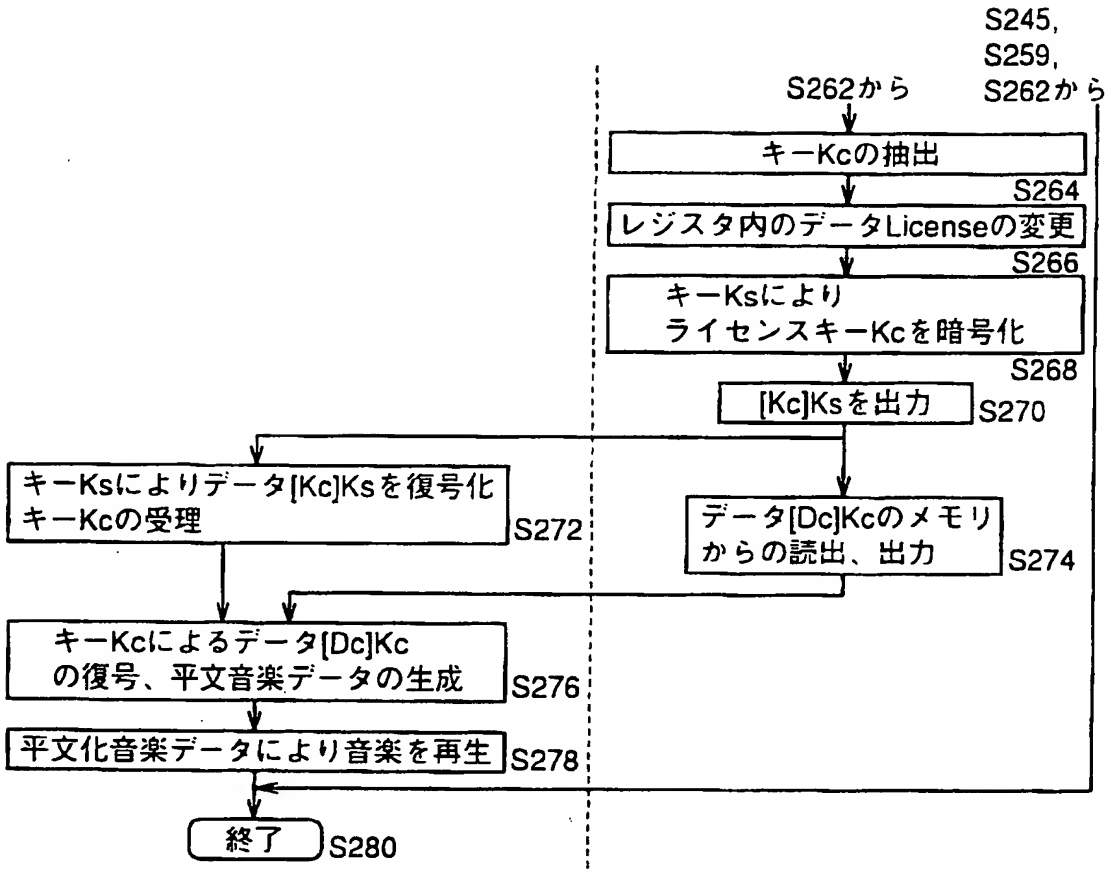

S245,
S259,
S262から
S262から
キーKcの抽出
S264
レジスタ内のデータLicenseの変更
S266
キーKsにより
ライセンスキーKcを暗号化
S268
[Kc]Ksを出力
S270
キーKsによりデータ[Kc]Ksを復号化
キーKcの受理
S272
データ[Dc]Kcのメモリ
からの読出、出力
S274
キーKcによるデータ[Dc]Kc
の復号、平文音楽データの生成
S276
平文化音楽データにより音楽を再生
S278
終了
S280

FIG.39

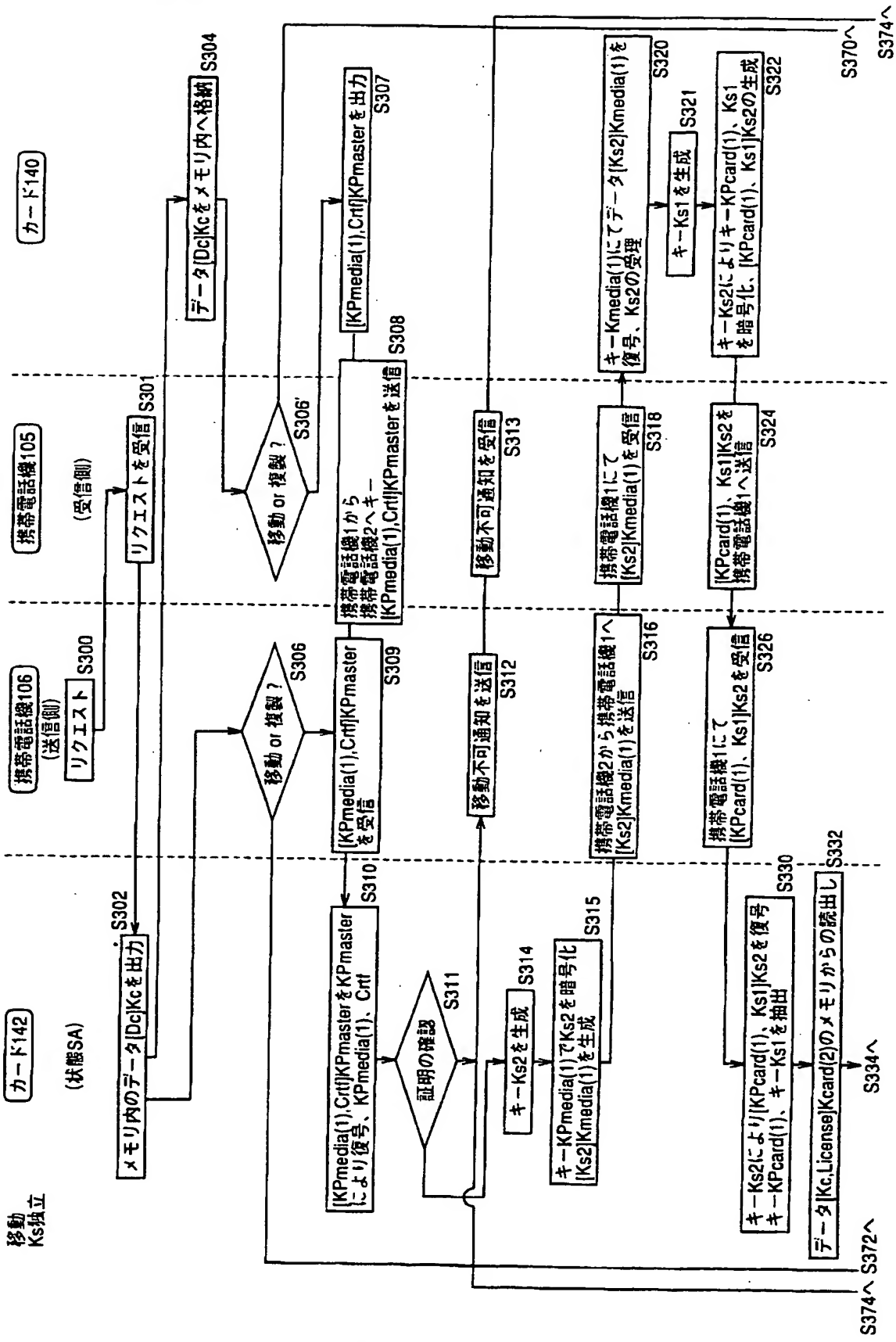

移動
Ks独立
カード142
(状態SA)
携帯電話機106
(送信側)
携帯電話機105
(受信側)
カード140
リクエスト
S300
リクエストを受信
S301
メモリ内のデータ[Dc]Kcを出力
S302
データ[Dc]Kcをメモリ内へ格納
S304
移動 or 複製 ?
S306
移動 or 複製 ?
S306'
[KPmedia(1),Crtf]KPmasterを受信
S309
[KPmedia(1),Crtf]KPmasterを出力
S307
携帯電話機1から携帯電話機2へキー[KPmedia(1),Crtf]KPmasterを送信
S308
[KPmedia(1),Crtf]KPmasterをKPmaster[KPmedia(1)]により復号、KPmedia(1)、Crtf
S310
証明の確認
S311
移動不可通知を送信
S312
移動不可通知を受信
S313
キーKs2を生成
S314
キーKPmedia(1)でKs2を暗号化[Ks2]Kmedia(1)を生成
S315
携帯電話機2から携帯電話機1へ[Ks2]Kmedia(1)を送信
S316
携帯電話機1にて[Ks2]Kmedia(1)を受信
S318
キーKmedia(1)にてデータ[Ks2]Kmedia(1)を復号、Ks2の受理
S320
キーKs1を生成
S321
キーKs2によりキーKPcard(1)、Ks1を暗号化、[KPcard(1)、Ks1]Ks2の生成
S322
[KPcard(1)、Ks1]Ks2を携帯電話機1へ送信
S324
携帯電話機1にて[KPcard(1)、Ks1]Ks2を受信
S326
キーKs2により[KPcard(1)、Ks1]Ks2を復号キーKPcard(1)、キーKs1を抽出
S330
データ[Kc,License]Kcard(2)のメモリからの読出し
S332
S334へ
S370へ
S372へ
S374へ
S374へ

FIG.40

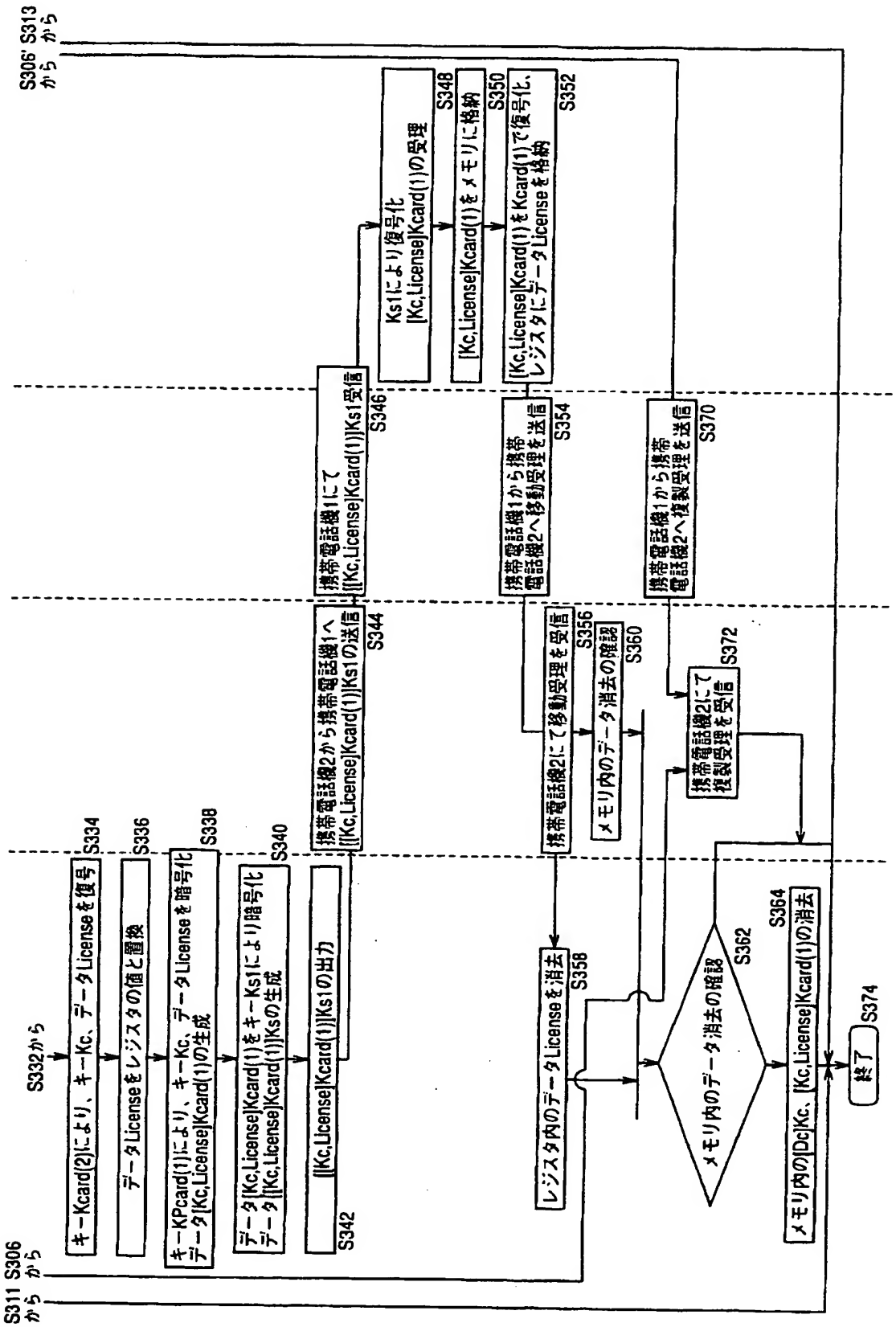

S311 S306 から
S332から
キーKcard(2)により、キーKc、データLicenseを復号
S334
データLicenseをレジスタの値と置換
S336
キーKPcard(1)により、キーKc、データLicenseを暗号化
データ[Kc,License]Kcard(1)の生成
S338
データ[Kc,License]Kcard(1)をキーKs1により暗号化
データ{[Kc,License]Kcard(1)}Ksの生成
S340
{[Kc,License]Kcard(1)}Ks1の出力
S342
携帯電話機2から携帯電話機1へ
{[Kc,License]Kcard(1)}Ks1の送信
S344
携帯電話機1にて
{[Kc,License]Kcard(1)}Ks1受信
S346
Ks1により復号化
[Kc,License]Kcard(1)の受理
S348
[Kc,License]Kcard(1)をメモリに格納
S350
[Kc,License]Kcard(1)をKcard(1)で復号化、
レジスタにデータLicenseを格納
S352
S306' S313 から
携帯電話機1から携帯電話機2へ移動受理を送信
S354
携帯電話機2にて移動受理を受信
S356
メモリ内のデータ消去の確認
S360
携帯電話機1から携帯電話機2へ複製受理を送信
S370
携帯電話機2にて複製受理を受信
S372
レジスタ内のデータLicenseを消去
S358
メモリ内のデータ消去の確認
S362
メモリ内の{Dc}Kc、[Kc,License]Kcard(1)の消去
S364
終了
S374

FIG.41

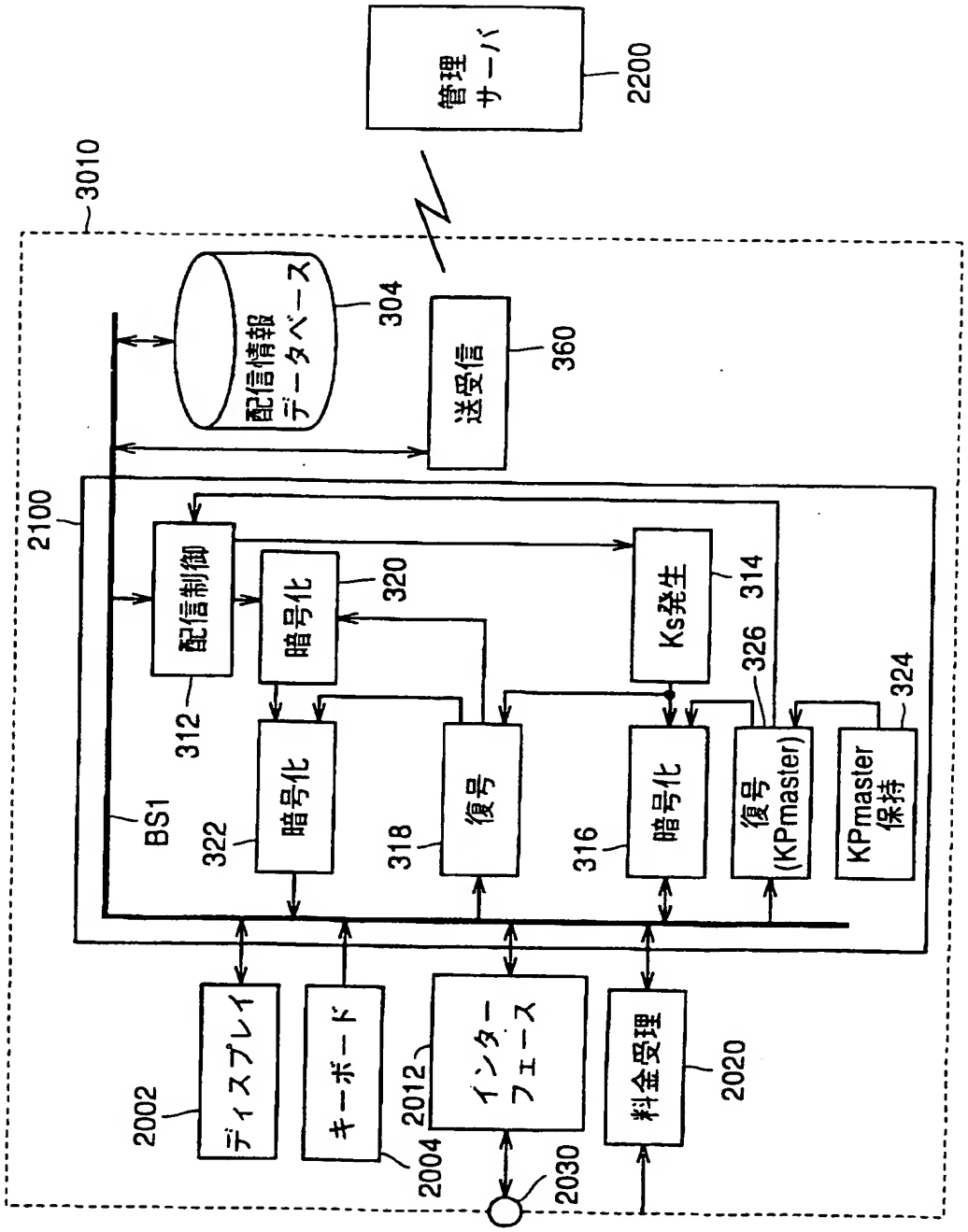

管理サーバ
2200
3010
配信情報データベース
304
送受信
360
2100
配信制御
312
暗号化
320
Ks発生
314
326
324
BS1
暗号化
322
復号
318
暗号化
316
復号(KPmaster)
KPmaster保持
ディスプレイ
2002
キーボード
2004
インターフェース
2012
料金受理
2020
2030

FIG.42

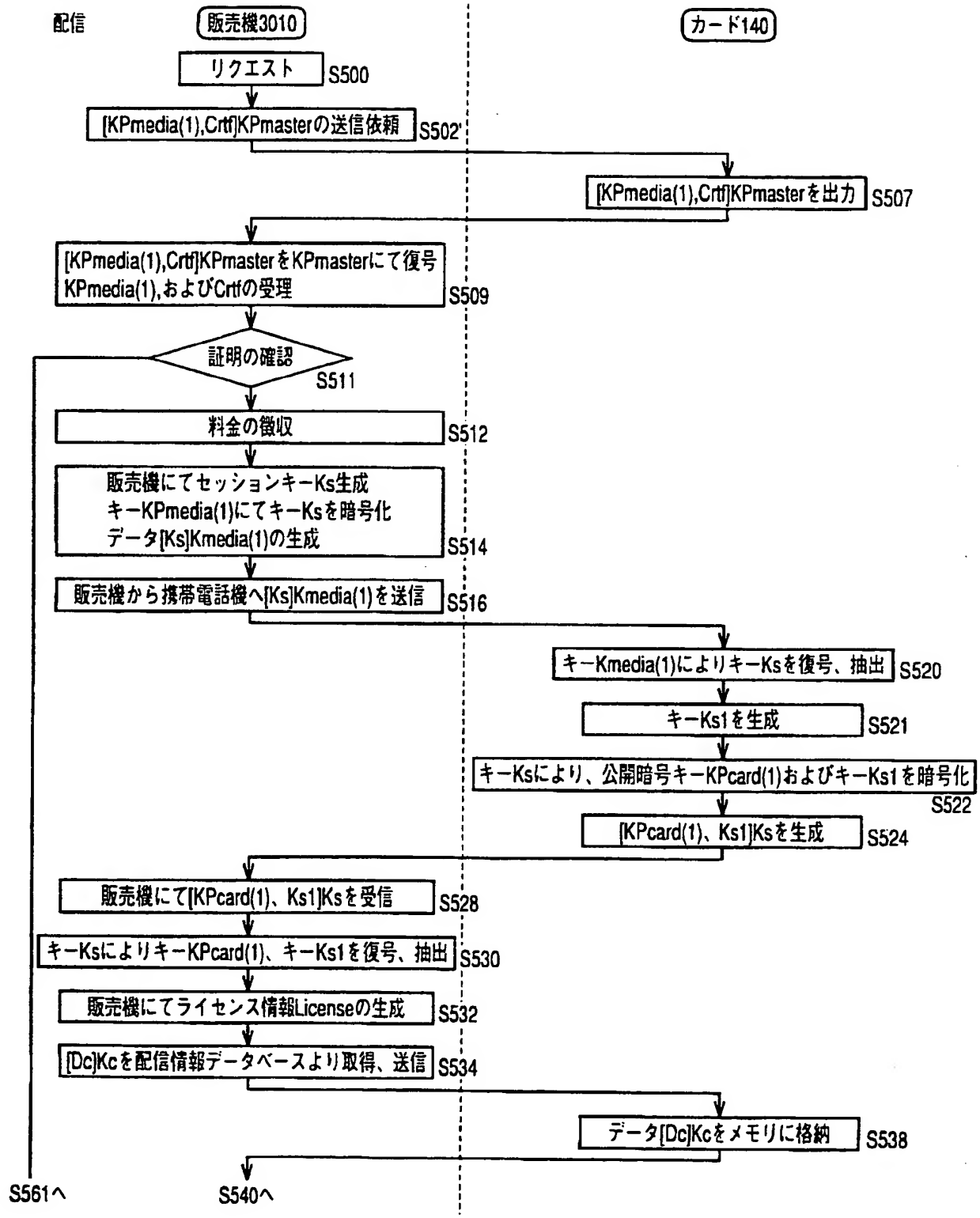
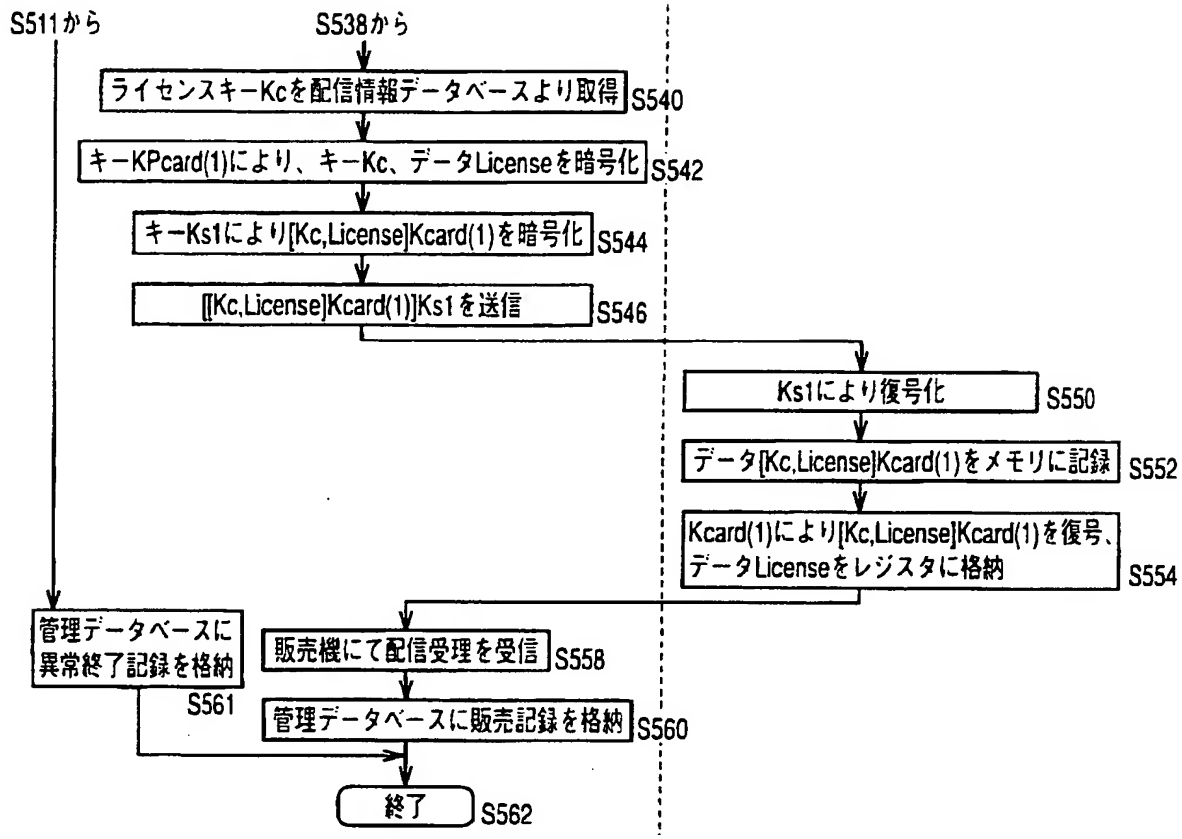

配信
販売機3010
カード140
リクエスト
S500
[KPmedia(1),Crtf]KPmasterの送信依頼
S502'
[KPmedia(1),Crtf]KPmasterを出力
S507
[KPmedia(1),Crtf]KPmasterをKPmasterにて復号
KPmedia(1),およびCrtfの受理
S509
証明の確認
S511
料金の徴収
S512
販売機にてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成
S514
販売機から携帯電話機へ[Ks]Kmedia(1)を送信
S516
キーKmedia(1)によりキーKsを復号、抽出
S520
キーKs1を生成
S521
キーKsにより、公開暗号キーKPcard(1)およびキーKs1を暗号化
S522
[KPcard(1)、Ks1]Ksを生成
S524
販売機にて[KPcard(1)、Ks1]Ksを受信
S528
キーKsによりキーKPcard(1)、キーKs1を復号、抽出
S530
販売機にてライセンス情報Licenseの生成
S532
[Dc]Kcを配信情報データベースより取得、送信
S534
データ[Dc]Kcをメモリに格納
S538
S561へ
S540へ

FIG.43


S511から
S538から
ライセンスキーKcを配信情報データベースより取得
S540
キーKPcard(1)により、キーKc、データLicenseを暗号化
S542
キーKs1により[Kc,License]Kcard(1)を暗号化
S544
[[Kc,License]Kcard(1)]Ks1を送信
S546
Ks1により復号化
S550
データ[Kc,License]Kcard(1)をメモリに記録
S552
Kcard(1)により[Kc,License]Kcard(1)を復号、データLicenseをレジスタに格納
S554
管理データベースに異常終了記録を格納
S561
販売機にて配信受理を受信
S558
管理データベースに販売記録を格納
S560
終了
S562

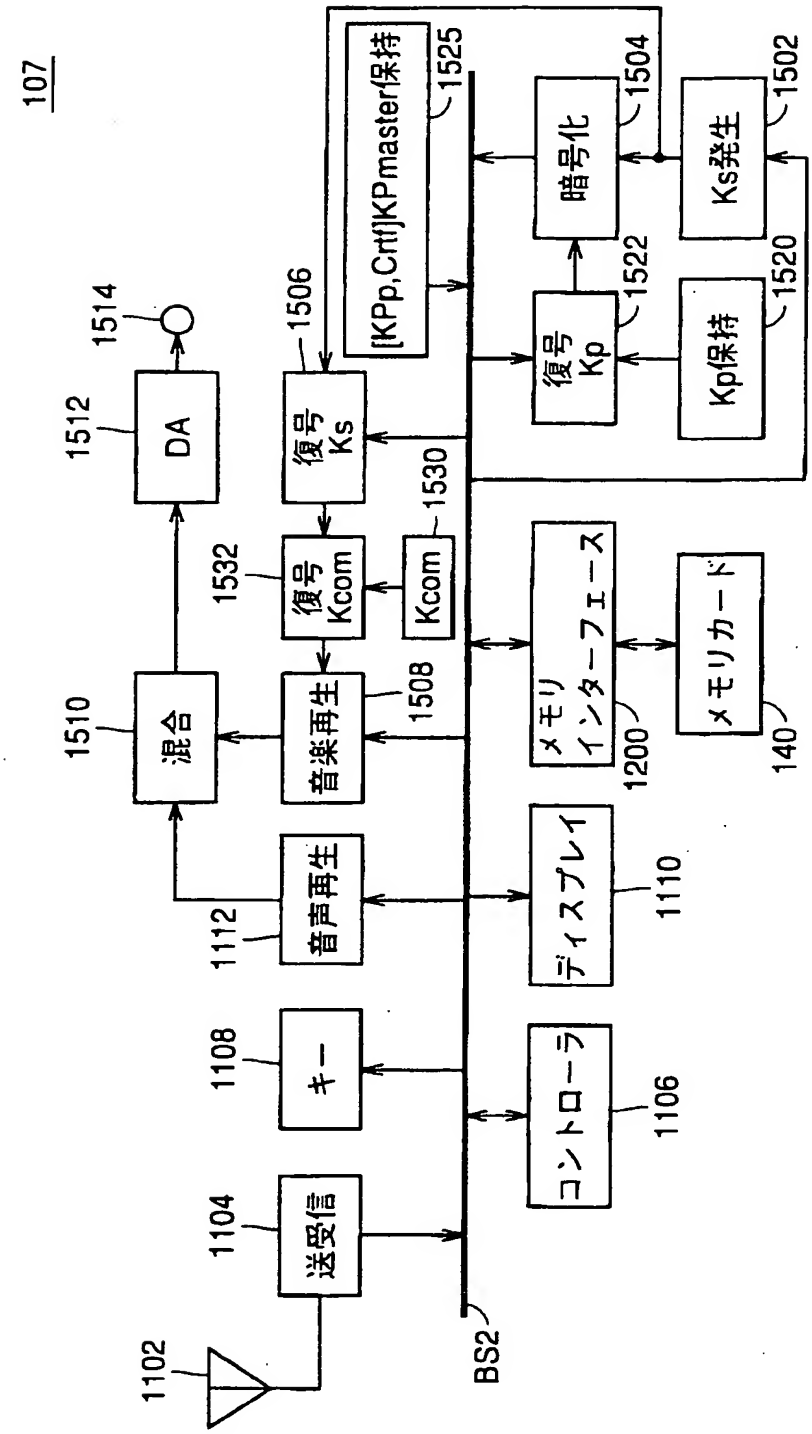

107
1102
1104
送受信
1108
キー
1112
音声再生
1510
混合
1512
DA
1514
1532
復号 Kcom
1508
音楽再生
1506
復号 Ks
[KPp,CntlJKPmaster保持
1525
1530
Kcom
BS2
コントローラ
1106
ディスプレイ
1110
メモリ インターフェース
1200
メモリカード
140
暗号化
1504
復号 Kp
1522
Kp保持
1520
Ks発生
1502

FIG.44

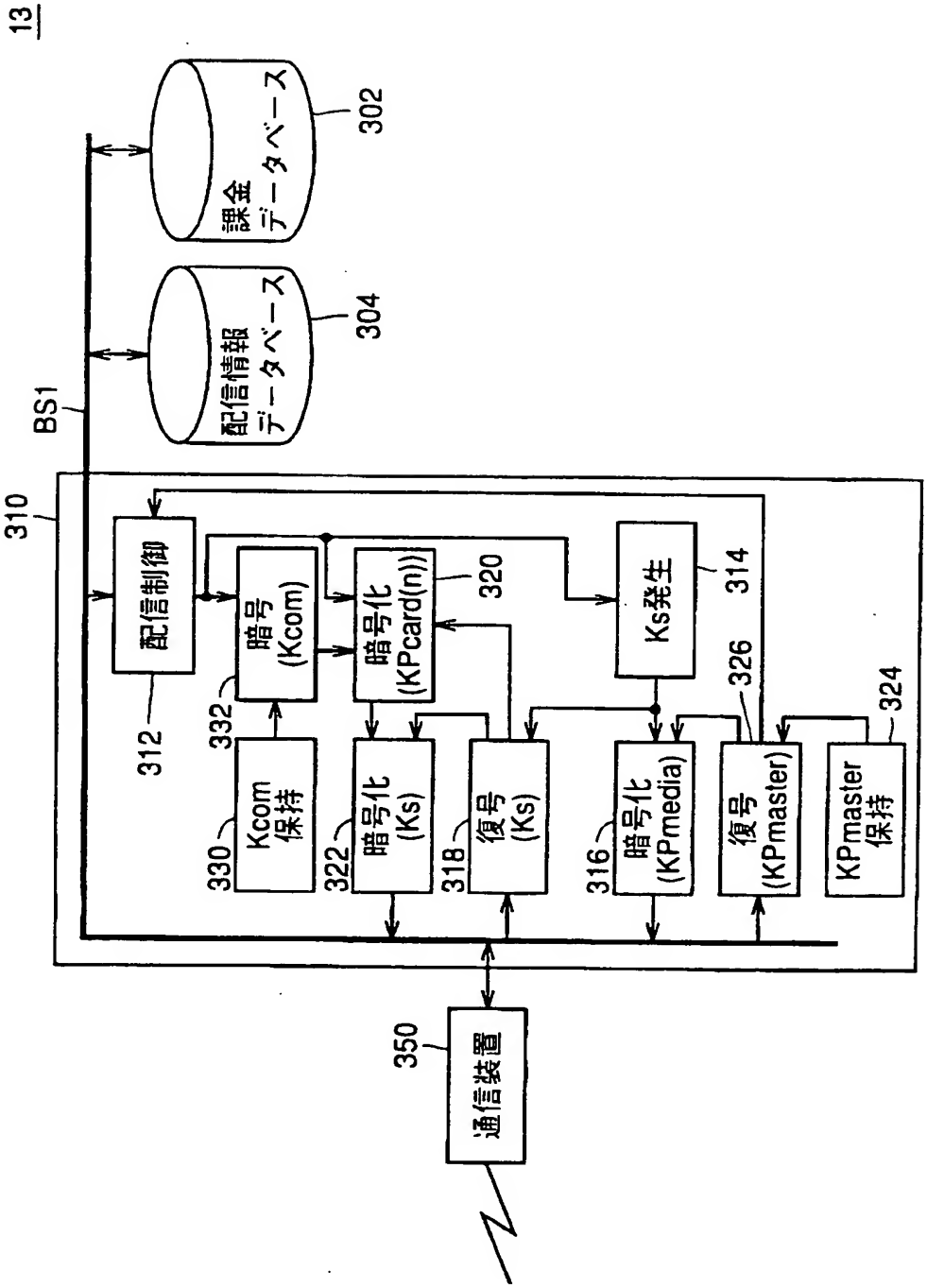

13
課金データベース
302
配信情報データベース
304
BS1
310
配信制御
312
暗号(Kcom)
332
暗号化((KPcard(n)))
320
Ks発生
314
Kcom保持
330
暗号化(Ks)
322
復号(Ks)
318
暗号化(KPmedia)
316
復号(KPmaster)
326
KPmaster保持
324
通信装置
350

FIG.45

FIG.46

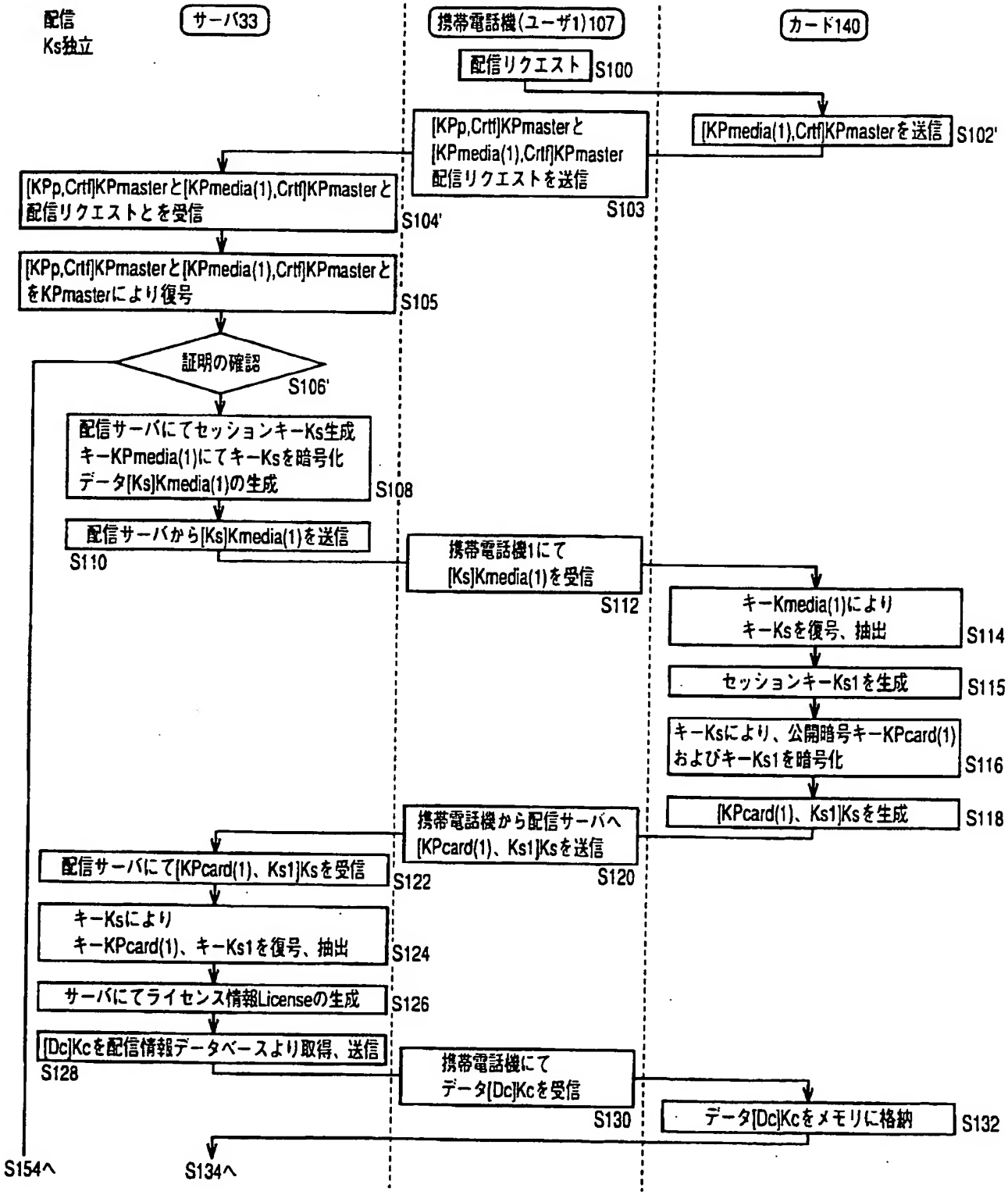

配信
Ks独立
サーバ33
携帯電話機(ユーザ1)107
カード140
配信リクエスト S100
[KPp,Crtf]KPmasterと[KPmedia(1),Crtf]KPmaster配信リクエストを送信 S103
[KPmedia(1),Crtf]KPmasterを送信 S102'
[KPp,Crtf]KPmasterと[KPmedia(1),Crtf]KPmasterと配信リクエストとを受信 S104'
[KPp,Crtf]KPmasterと[KPmedia(1),Crtf]KPmasterとをKPmasterにより復号 S105
証明の確認 S106'
配信サーバにてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成 S108
配信サーバから[Ks]Kmedia(1)を送信 S110
携帯電話機1にて[Ks]Kmedia(1)を受信 S112
キーKmedia(1)によりキーKsを復号、抽出 S114
セッションキーKs1を生成 S115
キーKsにより、公開暗号キーKPcard(1)およびキーKs1を暗号化 S116
[KPcard(1)、Ks1]Ksを生成 S118
携帯電話機から配信サーバへ[KPcard(1)、Ks1]Ksを送信 S120
配信サーバにて[KPcard(1)、Ks1]Ksを受信 S122
キーKsによりキーKPcard(1)、キーKs1を復号、抽出 S124
サーバにてライセンス情報Licenseの生成 S126
[Dc]Kcを配信情報データベースより取得、送信 S128
携帯電話機にてデータ[Dc]Kcを受信 S130
データ[Dc]Kcをメモリに格納 S132
S154へ
S134へ

FIG.47

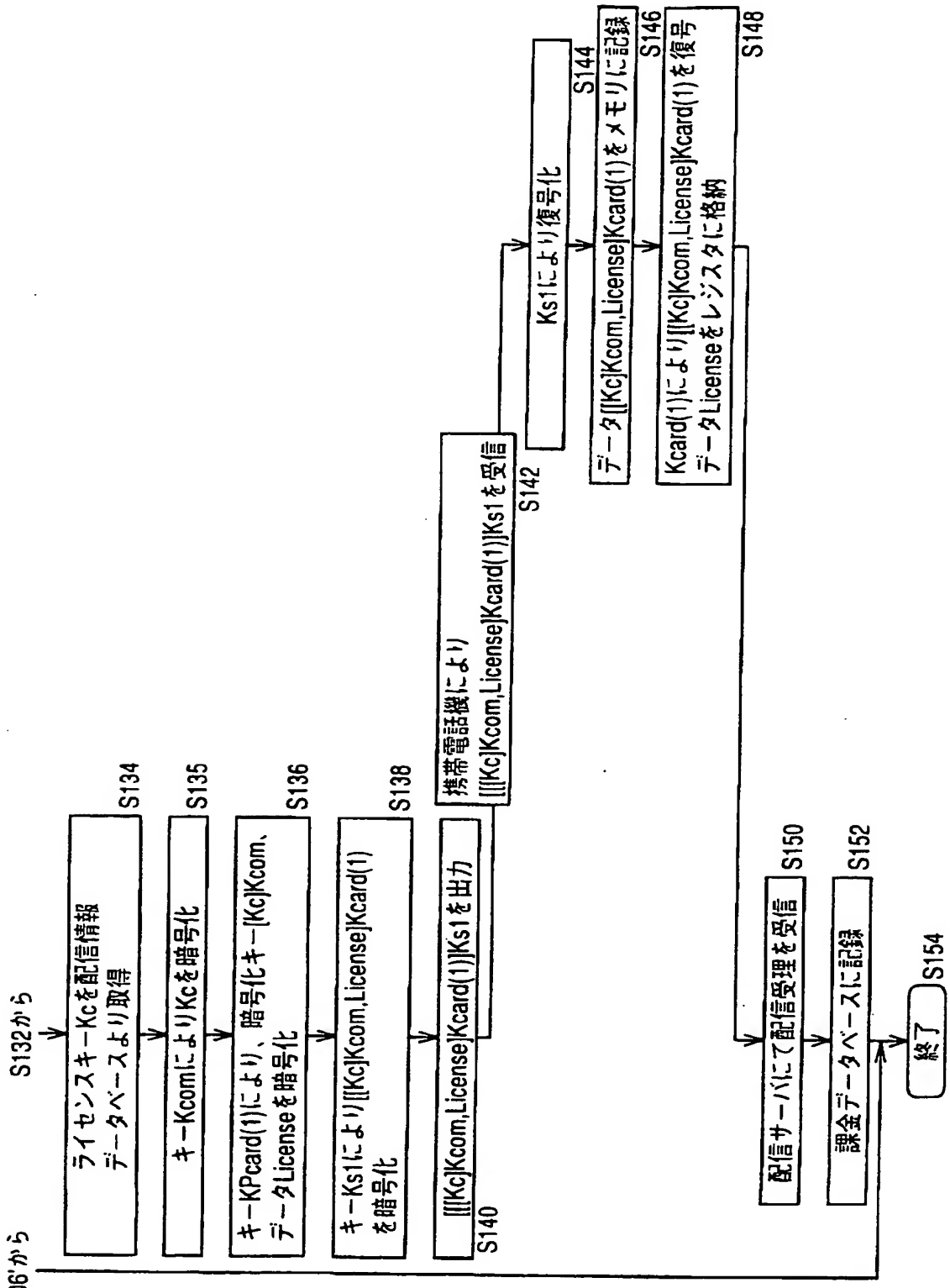

S106'から
S132から
ライセンスキーKcを配信情報データベースより取得
S134
キーKcomにより Kcを暗号化
S135
キーKPcard(1)により、暗号化キー[Kc]Kcom、データLicenseを暗号化
S136
キーKs1により[[Kc]Kcom,License]Kcard(1)を暗号化
S138
[[[Kc]Kcom,License]Kcard(1)]Ks1を出力
S140
携帯電話機により[[[Kc]Kcom,License]Kcard(1)]Ks1を受信
S142
Ks1により復号化
S144
データ[[Kc]Kcom,License]Kcard(1)をメモリに記録
S146
Kcard(1)により[[Kc]Kcom,License]Kcard(1)を復号
データLicenseをレジスタに格納
S148
配信サーバにて配信受理を受信
S150
課金データベースに記録
S152
終了
S154

FIG.48

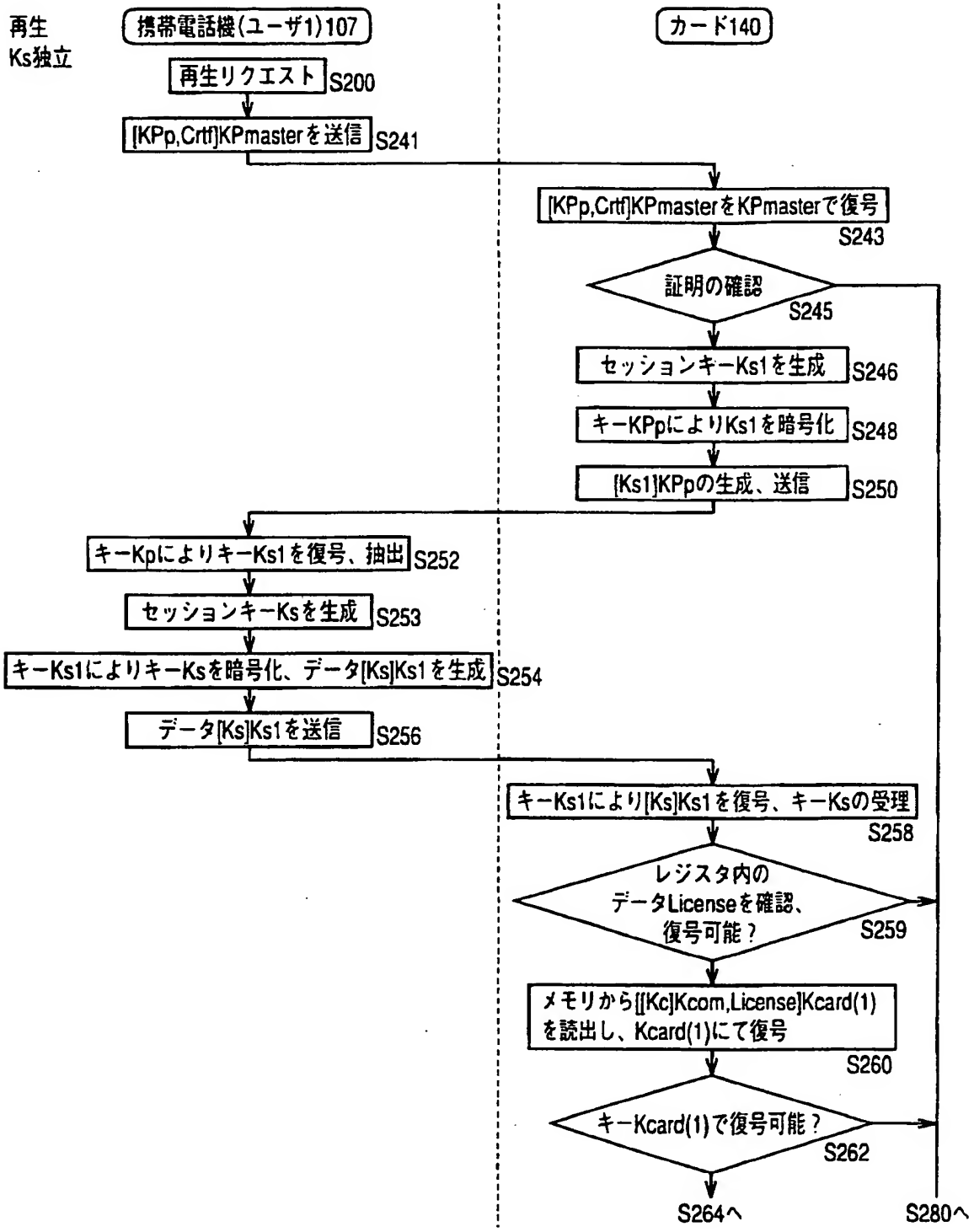

再生
Ks独立
携帯電話機(ユーザ1)107
カード140
再生リクエスト S200
[KPp,Crtf]KPmasterを送信 S241
[KPp,Crtf]KPmasterをKPmasterで復号 S243
証明の確認 S245
セッションキーKs1を生成 S246
キーKPpによりKs1を暗号化 S248
[Ks1]KPpの生成、送信 S250
キーKpによりキーKs1を復号、抽出 S252
セッションキーKsを生成 S253
キーKs1によりキーKsを暗号化、データ[Ks]Ks1を生成 S254
データ[Ks]Ks1を送信 S256
キーKs1により[Ks]Ks1を復号、キーKsの受理 S258
レジスタ内の
データLicenseを確認、
復号可能？ S259
メモリから[[Kc]Kcom,License]Kcard(1)
を読出し、Kcard(1)にて復号 S260
キーKcard(1)で復号可能？ S262
S264へ
S280へ

FIG.49

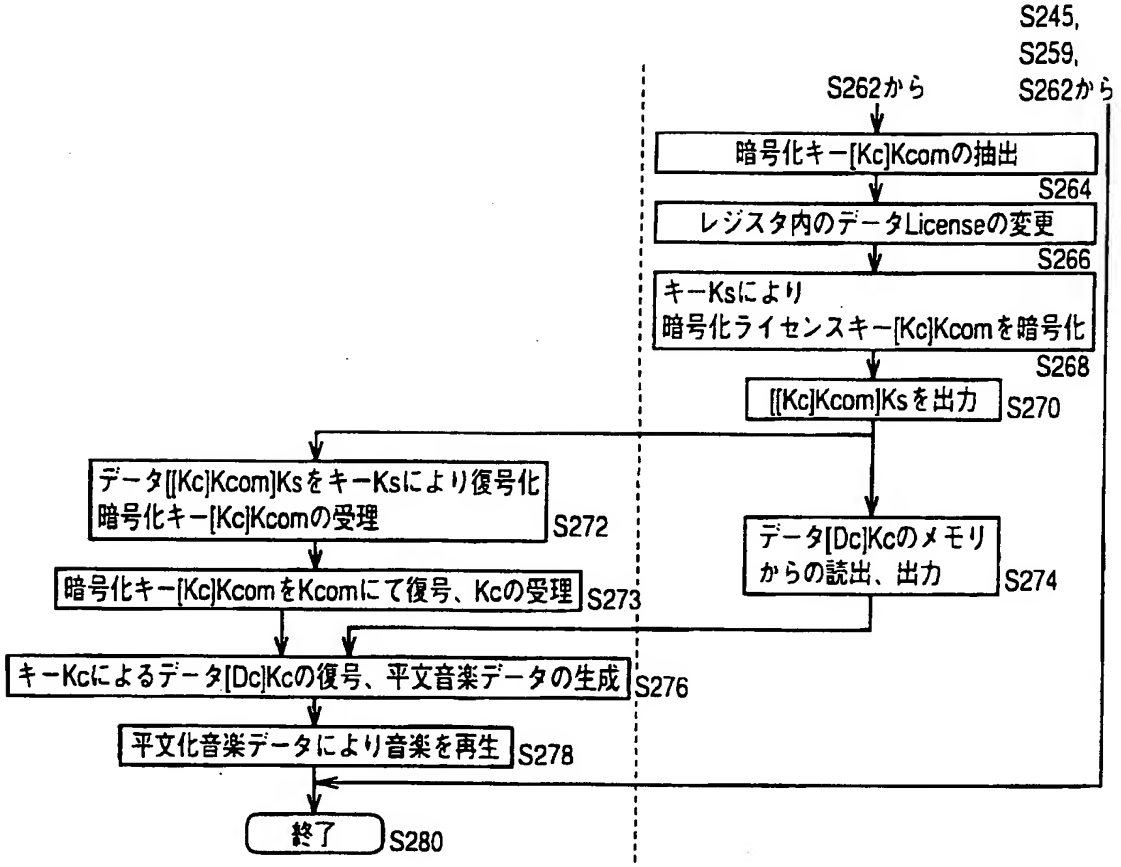

S245,
S259,
S262から
S262から
暗号化キー[Kc]Kcomの抽出
S264
レジスタ内のデータLicenseの変更
S266
キーKsにより
暗号化ライセンスキー[Kc]Kcomを暗号化
S268
[[Kc]Kcom]Ksを出力
S270
データ[[Kc]Kcom]Ksをキー Ksにより復号化
暗号化キー[Kc]Kcomの受理
S272
暗号化キー[Kc]KcomをKcomにて復号、Kcの受理
S273
データ[Dc]Kcのメモリ
からの読出、出力
S274
キーKcによるデータ[Dc]Kcの復号、平文音楽データの生成
S276
平文化音楽データにより音楽を再生
S278
終了
S280

FIG.50

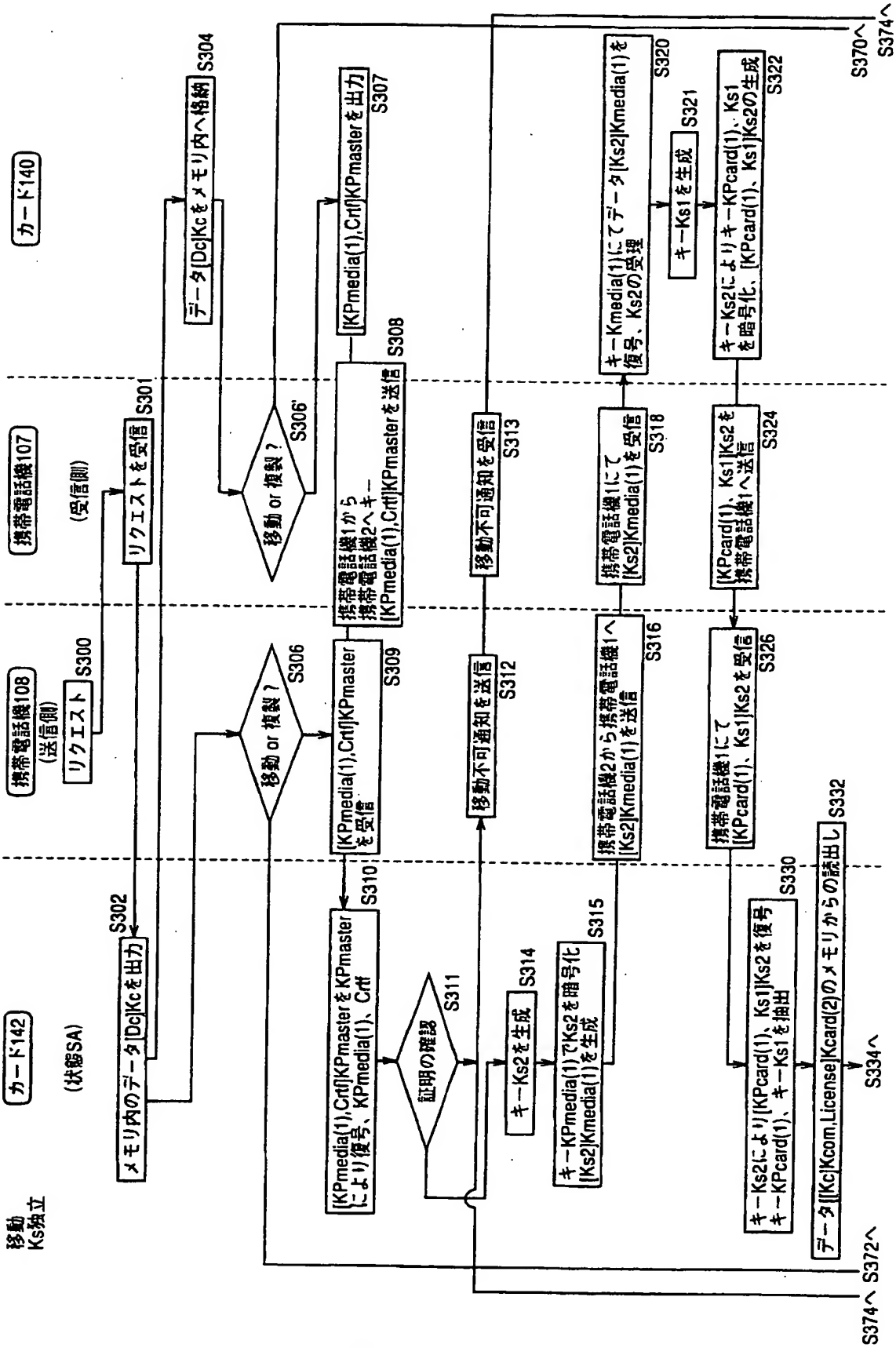
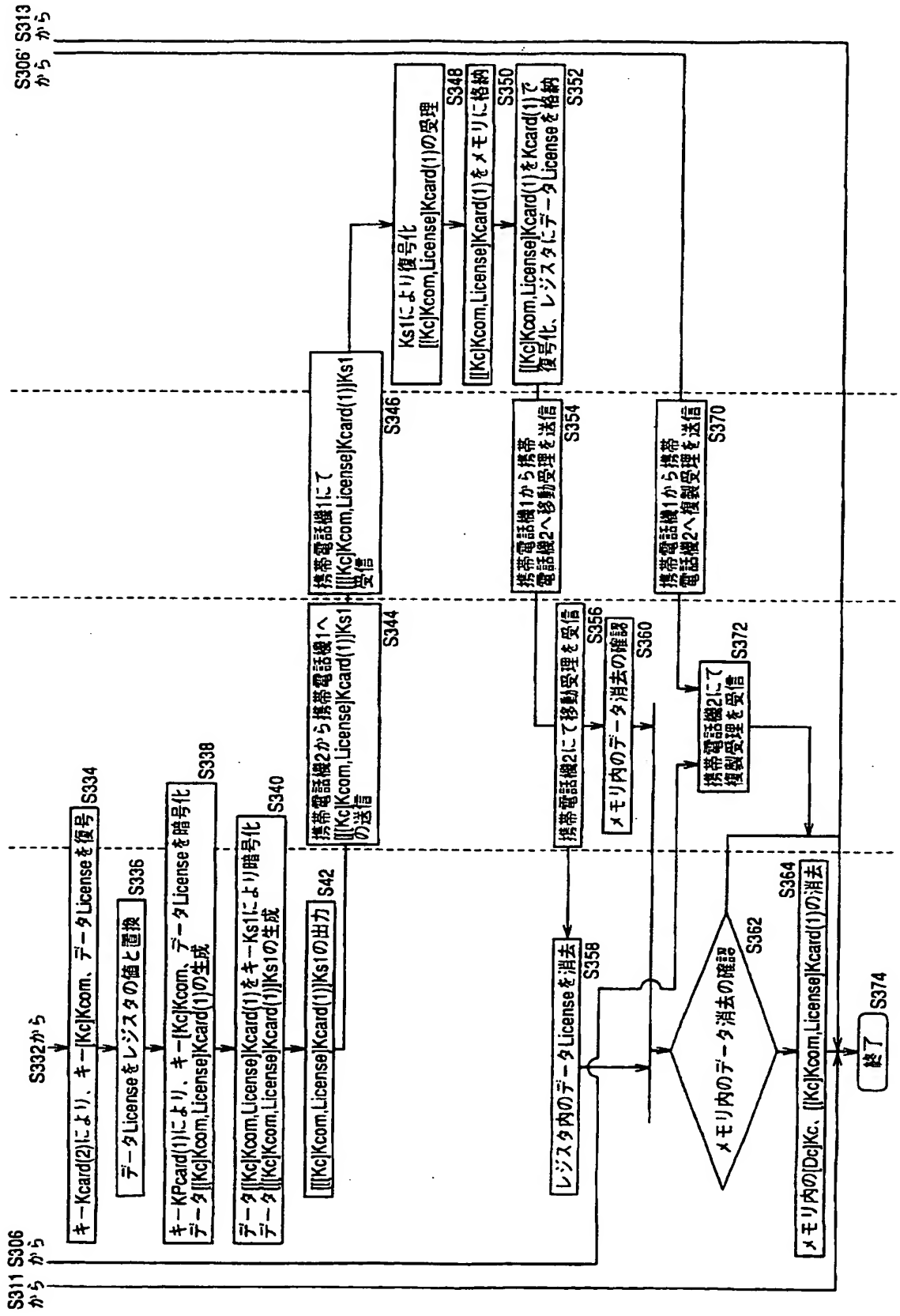

移動
Ks独立
カード142
(状態SA)
携帯電話機108
(送信側)
リクエスト
S300
メモリ内のデータ[Dc]Kcを出力
S302
リクエストを受信
S301
携帯電話機107
(受信側)
カード140
データ[Dc]Kcをメモリ内へ格納
S304
移動 or 複製 ?
S306
[KPmedia(1),Crtf]KPmasterを出力
S307
携帯電話機1から
携帯電話機2へキー
[KPmedia(1),Crtf]KPmasterを送信
S308
[KPmedia(1),Crtf]KPmaster
を受信
S309
移動 or 複製 ?
S306'
[KPmedia(1),Crtf]KPmaster
により復号、KPmedia(1)、Crtf
S310
証明の確認
S311
移動不可通知を送信
S312
移動不可通知を受信
S313
キーKs2を生成
S314
キーKpmedia(1)でKs2を暗号化
[Ks2]Kmedia(1)を生成
S315
携帯電話機2から携帯電話機1へ
[Ks2]Kmedia(1)を送信
S316
携帯電話機1にて
[Ks2]Kmedia(1)を受信
S318
キーKmedia(1)にてデータ[Ks2]Kmedia(1)を
復号、Ks2の受理
S320
キーKs1を生成
S321
キーKs2によりキーKPcard(1)、Ks1
を暗号化、[KPcard(1)、Ks1]Ks2の生成
S322
[KPcard(1)、Ks1]Ks2を
携帯電話機1へ送信
S324
携帯電話機1にて
[KPcard(1)、Ks1]Ks2を受信
S326
キーKs2により[KPcard(1)、Ks1]Ks2を復号
キーKPcard(1)、キーKs1を抽出
S330
データ[[Kc]Kcom,License]Kcard(2)のメモリからの読出し
S332
S334へ
S370へ
S372へ
S374へ
S374へ

FIG.51


S311 S306 から から
S332から
キーKcard(2)により、キー[Kc]Kcom、データLicenseを復号
S334
データLicenseをレジスタの値と置換
S336
キーKPcard(1)により、キー[Kc]Kcom、データLicenseを暗号化
データ[[Kc]Kcom,License]Kcard(1)の生成
S338
データ[[Kc]Kcom,License]Kcard(1)をキーKs1により暗号化
データ[[[Kc]Kcom,License]Kcard(1)]Ks1の生成
S340
[[[Kc]Kcom,License]Kcard(1)]Ks1の出力
S42
携帯電話機2から携帯電話機1へ
[[[Kc]Kcom,License]Kcard(1)]Ks1の送信
S344
携帯電話機1にて
[[[Kc]Kcom,License]Kcard(1)]Ks1受信
S346
Ks1により復号化
[[Kc]Kcom,License]Kcard(1)の受理
S348
[[Kc]Kcom,License]Kcard(1)をメモリに格納
S350
[[Kc]Kcom,License]Kcard(1)をKcard(1)で復号化、レジスタにデータLicenseを格納
S352
携帯電話機1から携帯電話機2へ移動受理を送信
S354
携帯電話機2にて移動受理を受信
S356
メモリ内のデータ消去の確認
S360
携帯電話機1から携帯電話機2へ複製受理を送信
S370
携帯電話機2にて複製受理を受信
S372
レジスタ内のデータLicenseを消去
S358
メモリ内のデータ消去の確認
S362
メモリ内の[Dc]Kc、[[Kc]Kcom,License]Kcard(1)の消去
S364
終了
S374
S306' S313 から から

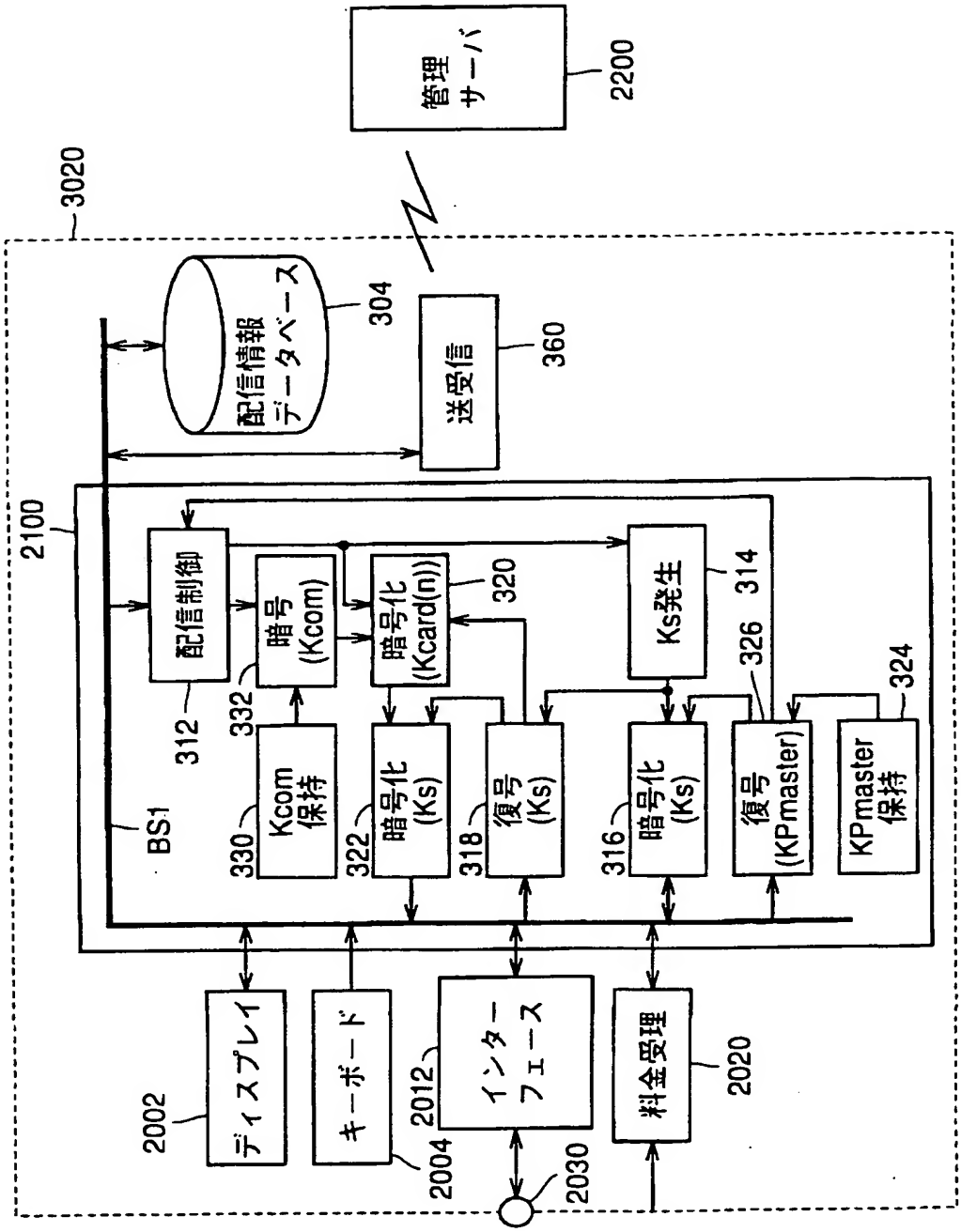

管理サーバ
2200
3020
配信情報データベース
304
送受信
360
2100
配信制御
312
暗号(Kcom)
332
暗号化(Kcard(n))
320
Ks発生
314
326
324
BS1
330
Kcom保持
322
暗号化(Ks)
318
復号(Ks)
316
暗号化(Ks)
復号(KPmaster)
KPmaster保持
2002
ディスプレイ
キーボード
2004
2012
インターフェース
2030
料金受理
2020

FIG.52

FIG.53

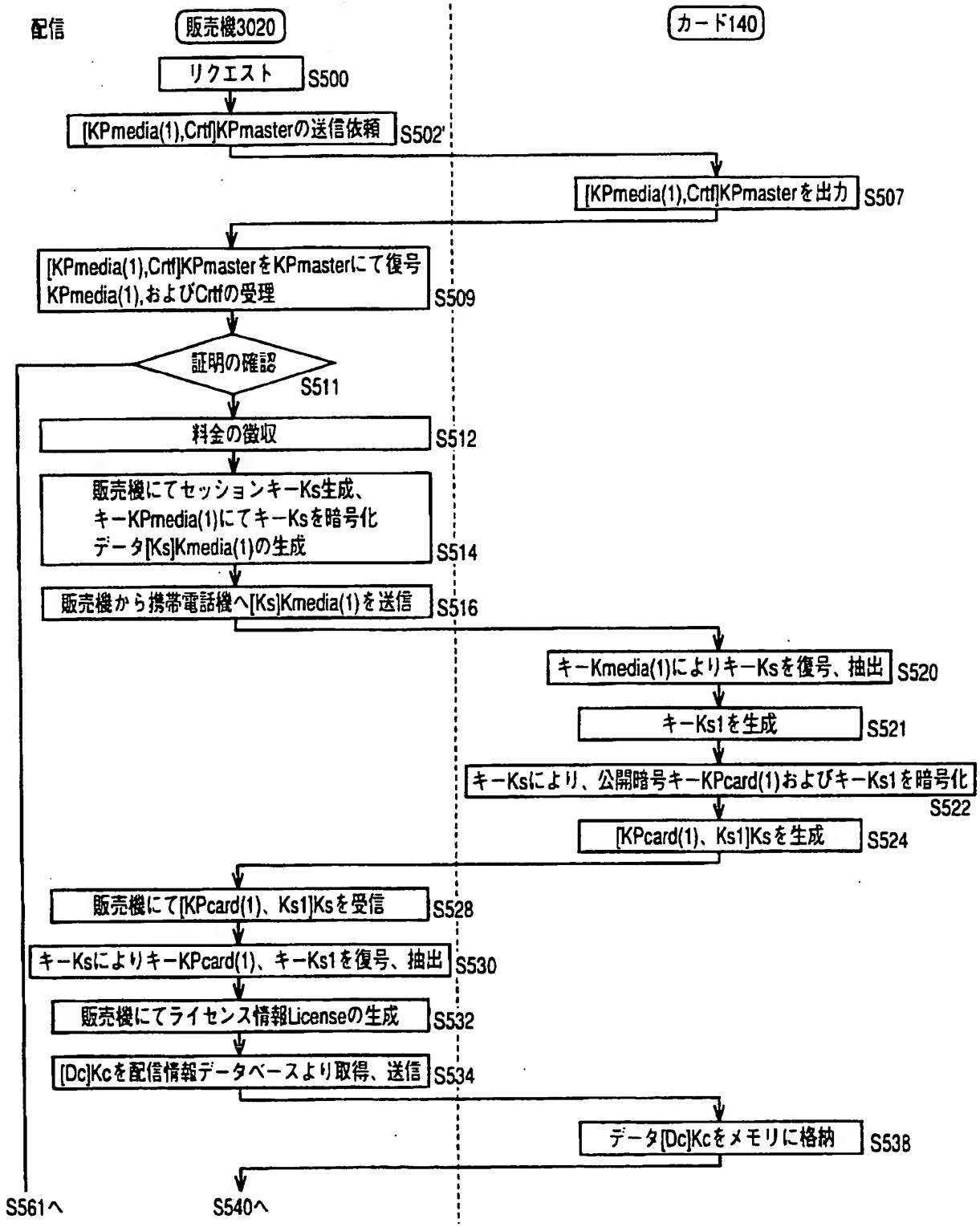

配信
販売機3020
カード140
リクエスト
S500
[KPmedia(1),Crtf]KPmasterの送信依頼
S502'
[KPmedia(1),Crtf]KPmasterを出力
S507
[KPmedia(1),Crtf]KPmasterをKPmasterにて復号
KPmedia(1),およびCrtfの受理
S509
証明の確認
S511
料金の徴収
S512
販売機にてセッションキーKs生成、
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成
S514
販売機から携帯電話機へ[Ks]Kmedia(1)を送信
S516
キーKmedia(1)によりキーKsを復号、抽出
S520
キーKs1を生成
S521
キーKsにより、公開暗号キーKPcard(1)およびキーKs1を暗号化
S522
[KPcard(1)、Ks1]Ksを生成
S524
販売機にて[KPcard(1)、Ks1]Ksを受信
S528
キーKsによりキーKPcard(1)、キーKs1を復号、抽出
S530
販売機にてライセンス情報Licenseの生成
S532
[Dc]Kcを配信情報データベースより取得、送信
S534
データ[Dc]Kcをメモリに格納
S538
S561へ
S540へ

FIG.54

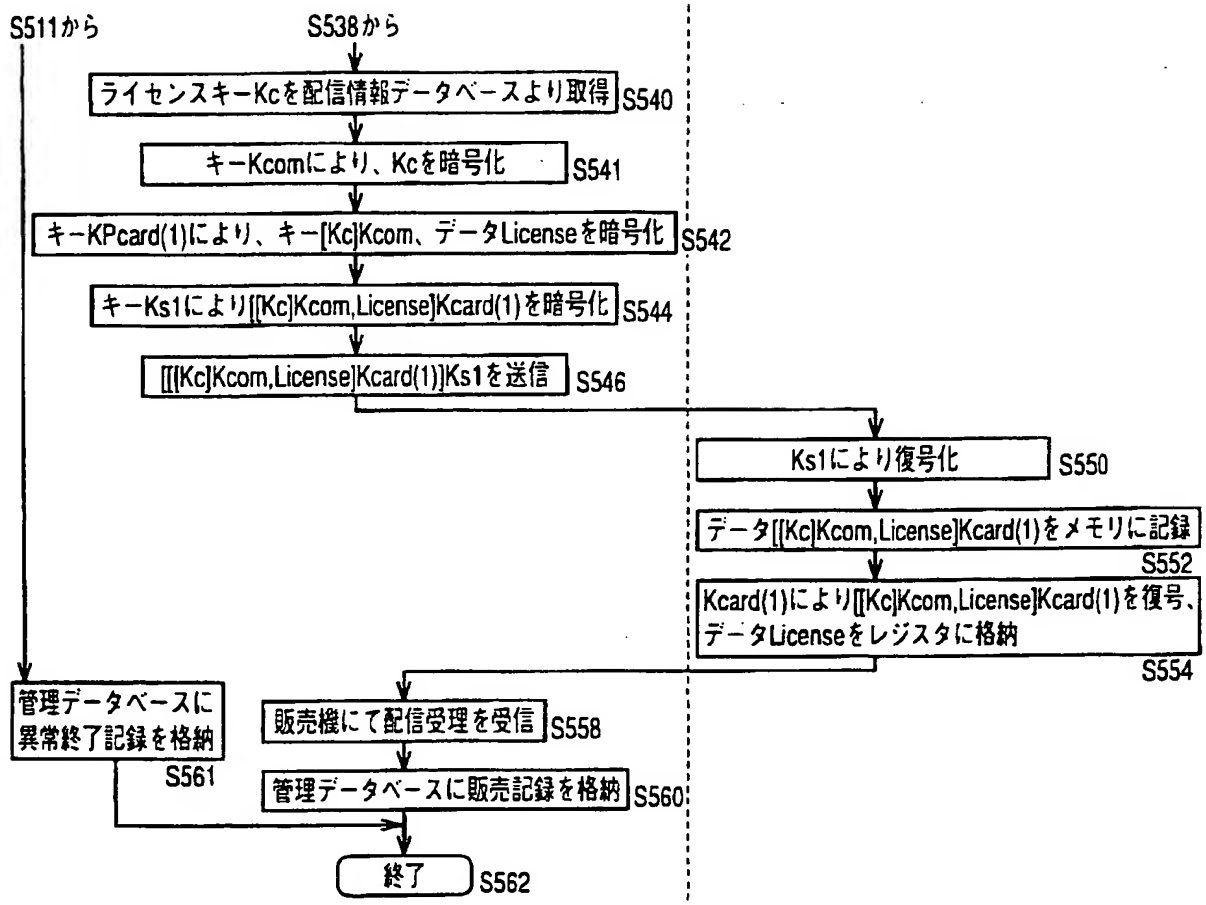

S511から
S538から
ライセンスキーKcを配信情報データベースより取得
S540
キーKcomにより、Kcを暗号化
S541
キーKPcard(1)により、キー[Kc]Kcom、データLicenseを暗号化
S542
キーKs1により[[Kc]Kcom,License]Kcard(1)を暗号化
S544
[[[Kc]Kcom,License]Kcard(1)]Ks1を送信
S546
Ks1により復号化
S550
データ[[Kc]Kcom,License]Kcard(1)をメモリに記録
S552
Kcard(1)により[[Kc]Kcom,License]Kcard(1)を復号、
データLicenseをレジスタに格納
S554
管理データベースに
異常終了記録を格納
S561
販売機にて配信受理を受信
S558
管理データベースに販売記録を格納
S560
終了
S562

FIG.55

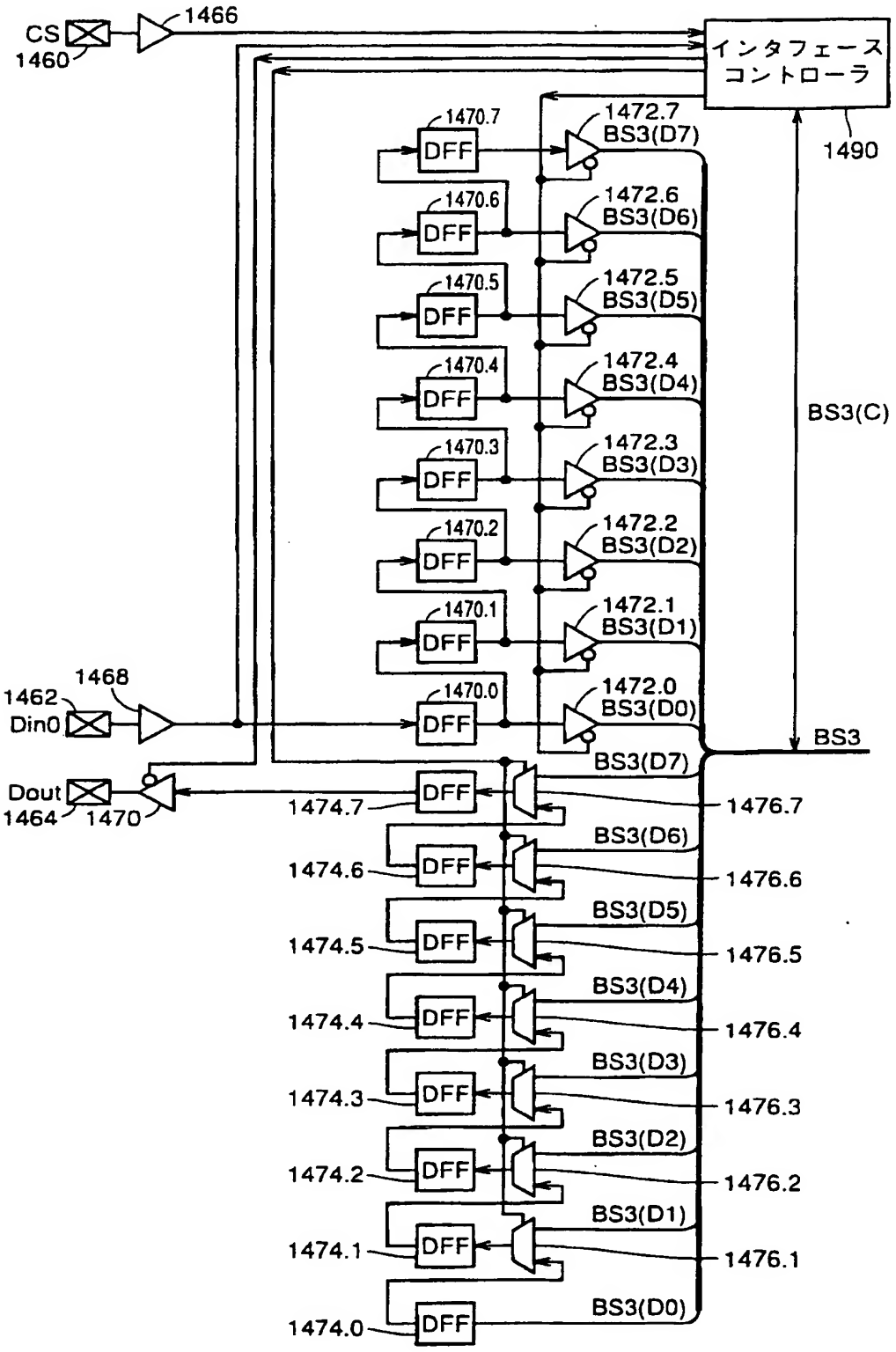
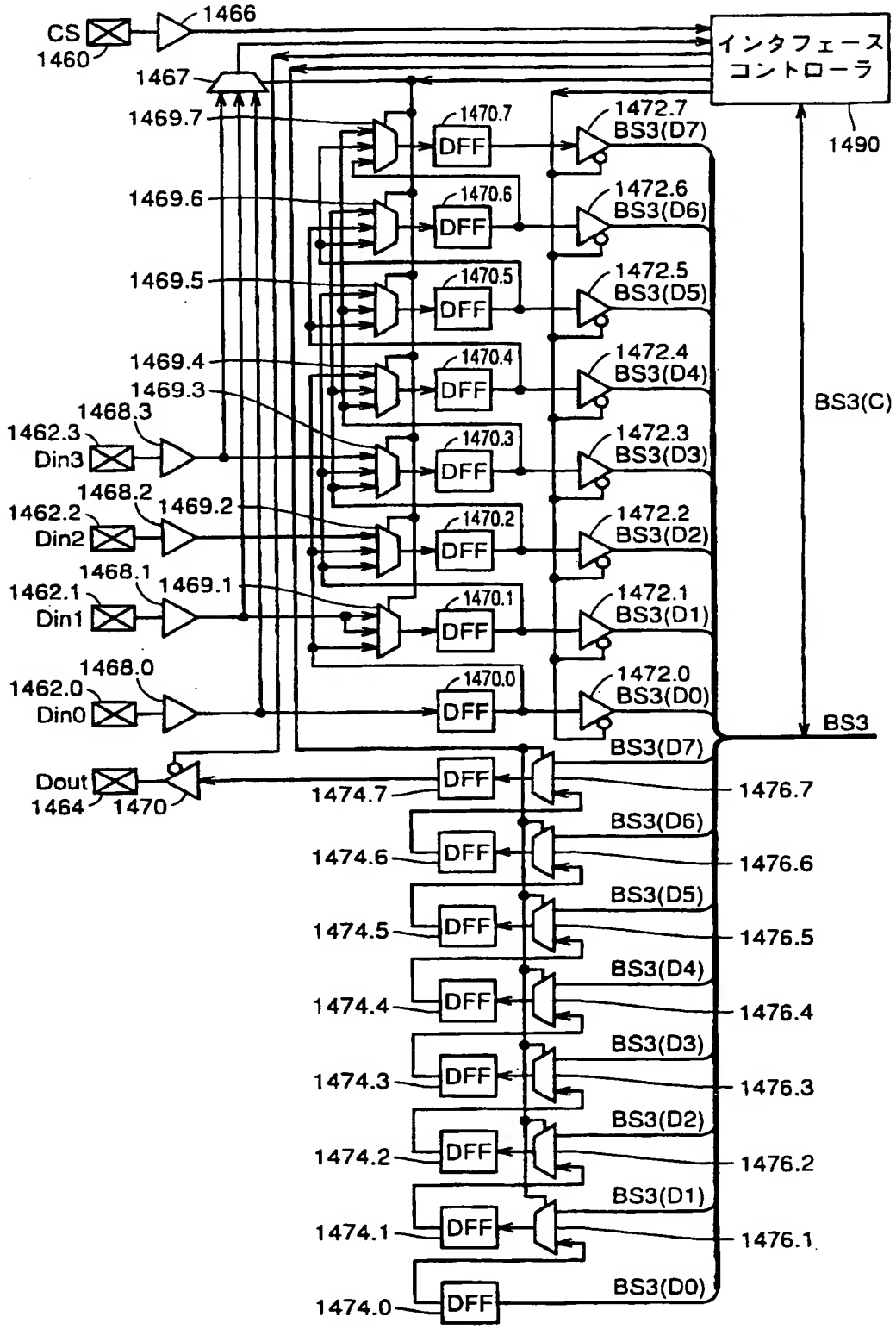

CS
1460
1466
インタフェース
コントローラ
1490
1470.7
DFF
1472.7
BS3(D7)
1470.6
1472.6
BS3(D6)
1470.5
1472.5
BS3(D5)
1470.4
1472.4
BS3(D4)
BS3(C)
1470.3
1472.3
BS3(D3)
1470.2
1472.2
BS3(D2)
1470.1
1472.1
BS3(D1)
1468
1462
Din0
1470.0
1472.0
BS3(D0)
BS3
BS3(D7)
Dout
1464
1470
1474.7
1476.7
BS3(D6)
1474.6
1476.6
BS3(D5)
1474.5
1476.5
BS3(D4)
1474.4
1476.4
BS3(D3)
1474.3
1476.3
BS3(D2)
1474.2
1476.2
BS3(D1)
1474.1
1476.1
BS3(D0)
1474.0

FIG.56


CS
1460
1466
1467
インタフェース
コントローラ
1490
1469.7
1469.6
1469.5
1469.4
1469.3
1469.2
1469.1
1468.3
1468.2
1468.1
1468.0
1462.3
Din3
1462.2
Din2
1462.1
Din1
1462.0
Din0
Dout
1464
1470
DFF
1470.7
1470.6
1470.5
1470.4
1470.3
1470.2
1470.1
1470.0
1472.7
BS3(D7)
1472.6
BS3(D6)
1472.5
BS3(D5)
1472.4
BS3(D4)
1472.3
BS3(D3)
1472.2
BS3(D2)
1472.1
BS3(D1)
1472.0
BS3(D0)
BS3(C)
BS3
1474.7
1474.6
1474.5
1474.4
1474.3
1474.2
1474.1
1474.0
1476.7
1476.6
1476.5
1476.4
1476.3
1476.2
1476.1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/05770

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G10K15/02, G06F15/00, G06F17/60, H04L9/08, H04L9/10, G06K19/00, H04H1/00, H04M3/42, H04M3/493, H04M11/08, G10L19/00, G06F13/00, H04L12/22, H04L12/58
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G10K15/00-15/06, G10L19/00-19/14, H04L9/00-9/38, G09C1/00-5/00, G06F12/00, G06F12/14, G06K19/00, H04M11/00-11/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1995 Toroku Jitsuyo Shinan Koho 1994-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
INSPEC (DIALOG)
WPI (DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP, 561685, A2 (FUJITSU LIMITED), 22 September, 1993 (22.09.93), Full text, all drawings & US, 5392351, A & US, 5555304, A & US, 5796824, A & JP, 5-257816, A & JP, 3073590, B2	1-33
A	JP, 62-53042, A (Nippon Telegr. & Teleph. Corp. <NTT>), 07 March, 1987 (07.03.87), Full text, all drawings (Family: none)	1-33
A	JP, 8-186667, A (Matsushita Electric Ind. Co., Ltd.), 16 July, 1996 (16.07.96), Full text, all drawings (Family: none)	1-33
A	JP, 8-69419, A (Shimadzu Corporation), 12 March, 1996 (12.03.96), Full text, all drawings (Family: none)	1-33
E,A	JP, 11-328033, A (Fujitsu Limited), 30 November, 1999 (30.11.99), Full text, all drawings (Family: none)	1-33

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
10 November, 2000 (10.11.00)

Date of mailing of the international search report
21 November, 2000 (21.11.00)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATION EARCH REPORT

Int ›nal application No.
PCT/JP00/05770

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Nikkei Electronics, No.739, "Kogata Memory Card de Ongaku Chosakuken wo mamoru", 22 March, 1999(22.03.99), pp.49-53	1-33
A	Nikkei Electronics, No.728, "Bei Shuuhen Kiki Maker Oote ga, MP3 Keitei gata Player Hatsubai; Chosakuken Taisaku wa Tsuika sezu", 19 October, 1998 (19.10.98), pp.31-32	1-33
A	Nikkei Electronics, No.731, "Yogoreta Image Fusshoku nerau MP3 Gyoukai; Ongaku Haishin no Kaigi, 'Web noise' kara", 30 November, 1998 (30.11.98), pp.29-30	1-33

国際調査報告

国際出願番号　PCT／JP00／05770

A.　発明の属する分野の分類（国際特許分類（IPC））

Int Cl' G10K15／02, G06F15／00, G06F17／60, H04L9／08, H04L9／10, G06K19／00, H04H1／00, H04M3／42, H04M3／493, H04M11／08, G10L19／00, G06F13／00, H04L12／22, H04L12／58

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int Cl' G10K15／00～15／06, G10L19／00～19／14, H04L9／00～9／38, G09C1／00～5／00, G06F12／00, G06F12／14, G06K19／00, H04M11／00～11／08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1926～1995年
日本国公開実用新案公報　1971～2000年
日本国登録実用新案公報　1994～2000年
日本国実用新案登録公報　1996～2000年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

INSPEC (DIALOG)
WPI (DIALOG)

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	EP, 561685, A2 (FUJITSU LIMITED), 22.9月.1993 (22.09.93), 全文全図, &US, 5392351, A &US, 5555304, A &US, 5796824, A &JP, 5-257816, A &JP, 3073590, B2	1-33
A	JP, 62－53042, A (日本電信電話株式会社), 7.3月.1987 (07.03.87), 全文全図 (ファミリーなし)	1-33
A	JP, 8－186667, A (松下電器産業株式会社), 16.7月.1996 (16.07.96), 全文全図 (ファミリーなし)	1-33

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
10. 11. 00	21.11.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	松尾　淳一　印	5C　8842
	電話番号　03－3581－1101　内線　3540	

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　PCT／JP00／05770

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	ＪＰ，８－６９４１９，Ａ(株式会社島津製作所)，12.3月.1996(12.03.96)，全文全図(ファミリーなし)	1-33
E，A	ＪＰ，１１－３２８０３３，Ａ(富士通株式会社)，30.11月.1999(30.11.99)，全文全図(ファミリーなし)	1-33
A	日経エレクトロニクス，No.739，「小型メモリ・カードで音楽著作権を守る」，22.3月.1999(22.03.99)，p.49-53	1-33
A	日経エレクトロニクス，No.728，「米周辺機器メーカ大手が，ＭＰ３携帯型プレーヤ発売　著作権対策は付加せず」，19.10月.1998(19.10.98)，p.31-32	1-33
A	日経エレクトロニクス，No.731，「汚れたイメージ払拭ねらうＭＰ３業界 音楽配信の会議 Webnoise から」，30.11月.1998(30.11.98)，p.29-30	1-33